UiO : Matematisk institutt
Det matematisk-naturvitenskapelige fakultet

4-torsjonspunkter på elliptiske romkurver

Astri Strand Lindbæck

Masteroppgave, våren 2015

Innledning

I denne oppgaven ønsker vi å undersøke punkter på kurver der det tangerende hyperplanet snitter kurven med spesielt høy multiplisitet. I det projektive planet er hyperplanene linjer. I hvert punkt på en glatt, plan projektiv kurve kan vi finne en tangentlinje, men kun et endelig antall punkter har tangentlinje som snitter kurven med høyere multiplisitet enn 2. Et slikt punkt kjenner vi som et *vendepunkt* på kurven.

En *elliptisk kurve* er en glatt kurve E med genus $g_E = 1$. Ved et valg av et punkt på kurven som origo, utgjør punktene på E en gruppe.

I det projektive rommet $\mathbb{P}^3$ er hyperplanene plan. I hvert punkt på en glatt kurve i $\mathbb{P}^3$ finnes et plan som snitter kurven med multiplisitet minst 3. På en elliptisk romkurve vil de spesielle punktene vi skal telle opp være de der et plan tangerer kurven i punktet med multiplisitet 4. Vi skal vise at det finnes 16 slike punkter, kalt *hyperoskulerende punkter*. Det er mulig å plassere fire plan slik at de hver inneholder fire hyperoskulerende punkter. Disse fire planene danner et tetraeder som snitter den elliptiske kurven i kun de 16 hyperoskulerende punktene. I denne oppgaven kommer vi fram til følgende resultat:

> *Det finnes 713 tetraedere gjennom de 16 hyperoskulerende punktene på en elliptisk kurve i* $\mathbb{P}^3$.

Hvis vi kaller origo i gruppa av punkter på E for P_0, er et $n-torsjonspunkt$ et punkt P som er slik at $nP = P_0$. Vendepunktene på $E \subseteq \mathbb{P}^2$ er 3-torsjonspunkter, mens de hyperoskulerende punktene på $E \subseteq \mathbb{P}^3$ er 4-torsjonspunkter.

Oppgaven er strukturert på følgende måte:

I kapittel 1 definerer vi glatte projektive kurver og divisorer på dem. Et lineært system består av effektive lineært ekvivalente divisorer, og vi viser at en slik mengde definerer en avbildning av en kurve inn i projektivt rom.

I kapittel 2 introduserer vi Riemann-Roch-formelen som beskriver en sammenheng mellom graden til en divisor D på en kurve, kurvens genus og vek-

torromsdimensjonen dim $\widetilde{\mathcal{L}(D)}$. Denne brukes til å beskrive divisorklasser på elliptiske kurver, og til å beskrive en elliptisk kurve i $\mathbb{P}^3$.

I kapittel 3 beskriver vi gruppestrukturen på en elliptisk kurve. På en plan elliptisk kurve finnes en elegant geometrisk konstruksjon av binæroperasjonen av punktene i gruppa, mens man generelt kan bruke divisorklasser av grad null for å definere addisjonen. Kapitlet avsluttes med to viktige resultat: dersom origo velges til å være et vendepunkt i $\mathbb{P}^2$, vil tre punkter på en elliptisk kurve i planet adderes til null hvis og bare hvis de ligger på linje. Dersom origo velges til å være et hyperoskulerende punkt i $\mathbb{P}^3$, vil fire punkter på en elliptisk romkurve adderes til null hvis og bare hvis de ligger i samme plan.

I kapittel 4 ser vi først på Hurwitz' formel for sammenhengen mellom genusen til to kurver og graden til en avbildning mellom dem. I denne formelen finner vi et ledd som er definerert som *ramifikasjonen* til avbildningen. Deretter vil vi bruke Hurwitz' formel for å finne antall vendepunkter på en glatt, plan kurve med gitt grad og genus. Vendepunktene er 3-torsjonspunkter, altså punkter P slik at $3P = P_0$.

I kapittel 5 bruker vi tilsvarende konstruksjoner som i kapittel 4 til å finne antall hyperoskulerende punkter på en glatt kurve i $\mathbb{P}^3$.

I kapittel 6 undersøker vi mengden av de hyperoskulerende punktene på en elliptisk romkurve E. Disse utgjør en undergruppe, kalt H_4, av gruppa som består av alle punktene på E. De hyperoskulerende punktene er 4-torsjonspunkter, altså punkter P slik at $4P = P_0$.

I kapittel 7 viser vi at H_4 er isomorf med gruppa $\mathbb{Z}_4 \times \mathbb{Z}_4$.

I kapittel 8 teller vi opp antall trekanter gjennom de ni 3-torsjonspunktene på en elliptisk kurve i $\mathbb{P}^2$. Disse punktene på kurven utgjør en gruppe som er isomorf med $\mathbb{Z}_3 \times \mathbb{Z}_3$. Sammen med resultatet som sier at tre punkter ligger på samme linje hvis og bare hvis de adderes til null, brukes denne isomorfien til å telle opp fire mulige trekanter gjennom vendepunktene på E i $\mathbb{P}^2$.

I kapittel 9 teller vi opp antall tetraedere gjennom 4-torsjonspunktene på en elliptisk kurve i $\mathbb{P}^3$. Siden H_4 er isomorf med $\mathbb{Z}_4 \times \mathbb{Z}_4$, og fire punkter i samme plan adderes til null, bruker vi kun addisjon av elementene i $\mathbb{Z}_4 \times \mathbb{Z}_4$ for å telle opp antall tetraedere.

I kapittel 10 går vi gjennom den geometriske konstruksjonen som ved et valg av origo i H_4, bestemmer hvilke av de andre hyperoskulerende punktene som er 4-torsjonspunkter, og hvilke som faktisk er 2-torsjonspunkter.

Takk til

Det er mange jeg har lyst til å takke i forbindelse med skrivingen av denne masteroppgaven.

Den første og absolutt største takken går til min veileder professor Kristian Ranestad. Din tålmodighet og forklaringsevne har gjort at jeg har kommet meg helskinnet og styrket gjennom en på forhånd ganske utenkelig prosess. Jeg kunne verken bedt om et bedre tema eller en bedre veileder.

Tusen takk til Fredrik Meyer og Karoline Moe for korrekturlesing og uvurderlige råd og kommentarer. Karoline fortjener en ekstra stor takk for å ha vært en støtte gjennom hele min tid på Blindern. De mange forvirrende møtene med algebraisk geometri har blitt litt lettere å takle etter en kaffepause med deg.

Videre vil jeg gjerne takke mine medstudenter i sjette etasje i Niels Henrik Abels Hus. Jeg har alltid kunnet lufte tanker og frustrasjoner hos dere, og dere har alltid vært behjelpelige og forståelsesfulle. Jeg vil gjerne nevne Pia spesielt, som har vært en god venninne, samarbeidspartner og støtte, både på og utenfor Blindern. I tillegg vil jeg gjerne rette en takk til de mange dyktige foreleserne jeg har hatt ved NTNU og UiO. Spesielt har førsteamanuensis Heidi Dahl og professor Petter Andreas Bergh styrket min interesse for matematikk.

Til slutt vil jeg gi en stor takk til familien min, og spesielt til min kjære samboer Pål. Selv om du kanskje ikke har kunnet hjelpe meg noe med innholdet, hadde faktisk ikke denne masteroppgaven vært til hvis det ikke var for deg.

Innhold

Kapittel 1

Divisorer og lineære systemer

I dette kapitlet vil vi definere projektive kurver, divisorer og lineære systemer. Kapitlet avsluttes med en forklaring av hvordan et lineært system definerer en avbildning av en kurve inn i projektiv rom.

1.1 Projektive kurver

Når vi i denne oppgaven skal omtale generelle og spesielle kurver, og generelle og spesielle punkter på dem, vil det være hensiktsmessig å først gi noen forklaringer og definisjoner:

Kurvene, linjene, planene og flatene vi skal undersøke og bruke, befinner seg alle i et komplekst projektivt rom. Det komplekse projektive planet $\mathbb{P}^2$ over $\mathbb{C}$ er definert som $\mathbb{C}^3 \setminus \{0\}/\sim$, der $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ dersom $(x_2, y_2, z_2) = (kx_1, ky_1, kz_1)$ for en konstant $k \in \mathbb{C}$. Alle punkter i $\mathbb{C}^3$ som kan skrives på formen (kx_1, ky_1, kz_1) er i ekvivalensklassen $(x_1 : y_1 : z_1)$, som er et punkt i det projektive planet. På tilsvarende måte defineres projektive rom av høyere dimensjon. For å forenkle notasjonen, skriver vi i her kun $\mathbb{P}^n$ i steden for $\mathbb{P}^n$ over $\mathbb{C}$.

Definisjon 1.1. En *projektiv kurve* er en mengde punkter i et projektivt rom $\mathbb{P}^n$ som utgjør nullpunktsmengden til $n-1$ homogene, ikke-konstante polynomer $F_1, \ldots, F_{n-1}$. Dette er altså punktene som er løsninger til likningssettet

$$\begin{aligned} F_1(x_0, \ldots, x_n) &= 0, \\ &\vdots \\ F_{n-1}(x_0, \ldots, x_n) &= 0. \end{aligned}$$

Definisjon 1.2. La en kurve i $\mathbb{P}^n$ være gitt av polynomene $F_1, \ldots, F_{n-1}$. Dersom et punkt $P = (x_0 : \ldots : x_n)$ på kurven er slik at alle de partiellderiverte $\frac{\partial F_i(P)}{\partial x_j}$, der $i \in [1, n-1]$ og $j \in [0, n]$, er null samtidig, er P et *singulært punkt*. Dersom det ikke finnes noen slike punkter, er kurven *ikkesingulær*, eller *glatt*.

Eksempel 1.3. La en kurve i $\mathbb{P}^2$ være gitt av $F(x, y, z) = x^2 + yz + z^2$. De partiellderiverte er

$$\frac{\partial f}{\partial x} = 2x, \quad \frac{\partial f}{\partial y} = z, \quad \frac{\partial f}{\partial z} = y + 2z.$$

Siden $(0 : 0 : 0) \notin \mathbb{P}^2$, vil ingen punkter være slik at alle de partiellderiverte er null samtidig. Dermed er kurven glatt.

Eksempel 1.4. La en kurve i $\mathbb{P}^2$ være gitt av $F(x, y, z) = zy^2 - x^3 - zx^2$. De partiellderiverte er

$$\frac{\partial f}{\partial x} = -3x^2 - 2zx, \quad \frac{\partial f}{\partial y} = 2zy, \quad \frac{\partial f}{\partial z} = y^2 - x^2.$$

Evaluerer vi de partiellderiverte i punktet $P = (0 : 0 : 1)$, får vi $\frac{\partial f(P)}{\partial x} = \frac{\partial f(P)}{\partial y} = \frac{\partial f(P)}{\partial z} = 0$. Kurven er altså singulær, og P er et singulært punkt.

En kurve vil i denne oppgaven alltid bety en ikkesingulær projektiv kurve.

Definisjon 1.5. En rasjonal funksjon på en projektiv kurve C er en funksjon $f = \frac{g}{h} : C \longrightarrow \mathbb{C}$, der g og h er homogene polynomer av samme grad. Mengden av alle rasjonale funksjoner på C utgjør funksjonskroppen $K(C)$.

Definisjon 1.6. Den diskrete valuasjonen $v_P : K(C) \longrightarrow \mathbb{Z}$ tar en rasjonal funksjon på kurven og tilordner den et heltall $v_P(f)$, slik at følgende er oppfylt for rasjonale funksjoner f og g:

- $v_P(fg) = v_P(f) + v_P(g)$ og $v_P\left(\frac{f}{g}\right) = v_P(f) - v_P(g)$.
- $v_P(f + g) \geq \min\{v_P(f), v_P(g)\}$.

I tillegg har valuasjonen følgende egenskaper:

- Dersom $v_P(f) > 0$ er P et nullpunkt for f.
- Dersom $v_P(f) < 0$ er P en pol for f. Da kaller vi verdien $-v_P(f)$ for *polordenen* til f.
- Dersom $v_P(f) = 0$, er $f(P) \neq 0$.
- $v_P(\lambda) = 0$ for en konstant $\lambda \in \mathbb{C}$.

Siden hvert punkt på kurven er ikke-singulært, er den lokale ringen $\mathcal{O}_{C,P}$ en diskret valuasjonsring:

$$\mathcal{O}_{C,P} = \{f \in K(C) \setminus \{0\} \mid v_P(f) \geq 0\} \cup \{0\} \subseteq K(C),$$

med maksimalt ideal

$$m_{C,P} = \{f \in \mathcal{O}_{C,P} \mid v_p(f) > 0\} = \{f \in \mathcal{O}_{C,P} \mid f(P) = 0\}.$$

Vi skal senere i oppgaven se på snittet mellom en linje og en kurve i $\mathbb{P}^2$. *Snittmultiplisiteten* mellom kurven $C \subseteq \mathbb{P}^2$ og en linje L i et punkt P er et heltall $I_P(C, L) \geq 0$. Dersom P ikke er i snittet mellom linja og kurven, er $I_P(C, L) = 0$. Dersom $P \in C \cap L$, vil $I_P(C, L)$ generelt være lik én, men hvis $I_P(C, L) \geq 2$, er L lik tangentlinja til kurven i P. Videre kan vi definere snittmultiplisitet mellom to kurver:

Definisjon 1.7. La C være en glatt kurve, D en kurve gitt av et polynom F, og la G være et polynom med grad lik $\deg(F)$ og slik at $\frac{F}{G} \in K(C)$. La i tillegg P' være et punkt på C slik at P' ikke er på kurven gitt av $G = 0$. Da defineres snittmultiplisiteten mellom C og D i P' som $I_{P'}(C, D) = v_{P'}(\frac{F}{G})$.

Når vi sier at et snitt mellom to kurver C og D inneholder et gitt antall punkter *telt med multiplisitet*, er dette antallet summen av snittmultiplisitetene, altså

$$\sum_{P \in C \cap D} I_P(C, D).$$

Definisjon 1.8 (Infleksjonspunkt)**.** La C være en kurve i $\mathbb{P}^2$, og P et punkt på C. Kall tangentlinja til C i P for $T_P(C)$. Dersom $I_P(C, T_P(C)) > 2$, er P et *infleksjonspunkt*.

En vanlig betegnelse på et infleksjonspunkt på en plan kurve, er *vendepunkt*.

Et viktig resultat om antall punkter i snittet mellom to kurver, er gitt i *Bézouts teorem* (Se [4, kapittel I.7]):

Teorem 1.9 (Bézout)**.** *La C og D være to distinkte kurver i $\mathbb{P}^2$ definert av to polynomer med grad henholdsvis c og d. Snittet mellom kurvene vil inneholde nøyaktig $c \cdot d$ punkter, telt med multiplisitet.*

1.2 Divisorer

En *divisor* D på en kurve C er gitt som en endelig sum

$$D = \sum_{P \in C} e_P P,$$

der $e_P \in \mathbb{Z}$, og $e_P = 0$ unntatt for endelig mange punkter $P \in C$ [4, kapittel II.6]. Videre er *graden* til en divisor definert som summen av koeffisientene:

$$\deg D = \sum_{P \in C} e_P.$$

Definisjon 1.10. En divisor er *effektiv* dersom $e_P \geq 0$ for alle $P \in C$. At en divisor er effektiv skrives $D \geq 0$.

Til en rasjonal funksjon f på C kan man assosiere en divisor $(f) = \sum_{P \in C} v_P(f)P$, der $v_P(f) \in \mathbb{Z}$ er valuasjonen til f i P. En slik divisor (f) kalles en *prinsipaldivisor*.

Lemma 1.11. $\deg(f) = 0$.

Bevis. La $f = \frac{g}{h}$ være en rasjonal funksjon på kurven C, der g og h har grad d. Kall kurven gitt av $g = 0$ for C_g og kurven gitt av $h = 0$ for C_h. For et punkt $P' \in C$ vil $v_{P'}(f) = I_{P'}(C, C_g) - I_{P'}(C, C_h)$. La graden til C være c. I følge teorem 1.9 vil snittet mellom C og C_g bestå av $c \cdot d$ punkter. Det samme vil snittet mellom C og C_h. Da vil graden til divisoren (f) være gitt som

$$\deg(f) = \sum_{P \in C} v_P(f) = \sum_{P \in C} I_P(C, C_g) - \sum_{P \in C} I_P(C, C_h) = cd - cd = 0. \quad \square$$

Siden $\deg(f) = 0$, vil ikke graden til en divisor D endre seg dersom man legger til en prinsipaldivisor. Dette er utgangspunktet for definisjonen av en type ekvivalensklasser av divisorer, kalt *divisorklasser*, med følgende ekvivalensrelasjon:

Definisjon 1.12. En divisor D' på kurven C er *lineært ekvivalent* med D dersom $D' = D + (f)$ for en rasjonal funksjon f på C. At D' og D er lineært ekvivalente skrives $D' \sim D$. Divisorklassen gitt av D er $[D]$.

En delmengde av alle divisorene som er lineært ekvivalente med D, er alle de *effektive* divisorene som er lineært ekvivalente med D.

Definisjon 1.13. Mengden av alle effektive divisorer lineært ekvivalente med D kaller vi et *komplett lineært system* $\mathcal{L}(D)$:

$$\mathcal{L}(D) = \{D + (f) \mid D + (f) > 0, f \in K(C)\}.$$

En divisor $D' \in \mathcal{L}(D)$ er altså gitt som

$$D' = \sum_{P \in C} e'_P P = \sum_{P \in C} (e_P + v_P(f))P.$$

Dersom vi har et snitt mellom en kurve C og en linje L, får vi en divisor på C, $\mathrm{div}_C(C \cap L)$, bestående av punktene i snittet. Denne divisoren blir altså definert som $\mathrm{div}_C(C \cap L) = \sum_{P \in C \cap L} e_P P$, der koeffisienten e_P er snittmultiplisiteten mellom C og L i P. Hvis C har grad d, vet vi av teorem 1.9 at snittet mellom C og L inneholder d punkter, telt med multiplisitet. Derfor

er $\deg(\mathrm{div}_C(C \cap L)) = d$. Tilsvarende kan vi se på divisorer gitt av snittet mellom for eksempel en romkurve og et plan.

Dersom vi har en divisor D, kan vi videre undersøke mengden av de rasjonale funksjonene f som gjør at divisoren $D' = D + (f)$ er effektiv. Vi kaller denne undermengden av $K(C)$ for $\widetilde{\mathcal{L}(D)}$:

$$\widetilde{\mathcal{L}(D)} = \{f \mid v_P(f) > -e_P \ \forall \ P \in C\} \subseteq K(C).$$

Lemma 1.14. *$\widetilde{\mathcal{L}(D)}$ er et vektorrom.*

Bevis. Siden $\widetilde{\mathcal{L}(D)}$ er en delmengde av vektorrommet bestående av alle rasjonale funksjoner på kurven, holder det å vise at $\widetilde{\mathcal{L}(D)}$ er lukket under addisjon og skalarmultiplikasjon. Ta $f, f' \in \widetilde{\mathcal{L}(D)}$. Av egenskapene for valuasjonen får vi $v_P(f + f') \geq min\{v_P(f), v_P(f')\}$. Da er også $f + f' \in \widetilde{\mathcal{L}(D)}$. For en konstant k har man at $v_P(kf) = v_P(k) + v_P(f) = 0 + v_P(f) = v_P(f)$, så kf er også i $\widetilde{\mathcal{L}(D)}$. □

Vi kan nå vise at $\mathcal{L}(D)$ har strukturen til et projektivt rom. Kall det tilhørende projektive rommet bestående av éndimensjonale underrom av $\widetilde{\mathcal{L}(D)}$ for $\mathbb{P}(\widetilde{\mathcal{L}(D)})$.

Korollar 1.15. $\mathbb{P}(\widetilde{\mathcal{L}(D)}) = \mathcal{L}(D)$.

Bevis. En $f \in \widetilde{\mathcal{L}(D)}$ som er ulik null vil generere et éndimensjonalt vektorrom $\langle f \rangle \subseteq \mathbb{P}(\widetilde{\mathcal{L}(D)})$. Det holder å vise at følgende avbildning er en bijeksjon:

$$\begin{aligned} \mathbb{P}(\widetilde{\mathcal{L}(D)}) &\longrightarrow \mathcal{L}(D), \\ \langle f \rangle &\mapsto D + (f). \end{aligned}$$

Ta to divisorer fra $\mathcal{L}(D)$, $D_1 = D + (f)$ og $D_2 = D + (g)$, slik at $D_1 = D_2$. Da har vi:

$$\begin{aligned} (f) &= (g), \\ v_P(f) &= v_P(g), \\ v_P(\frac{f}{g}) &= 0 \ \forall \ P \in C, \\ \frac{f}{g} &= \lambda \in \mathbb{C}, \\ f = \lambda g &\Rightarrow g \in \langle f \rangle, \\ \langle f \rangle &= \langle g \rangle. \end{aligned}$$

Dermed er avbildningen injektiv. Siden alle divisorene i $\mathcal{L}(D)$ er på formen $D + (f)$, for en $f \in \mathcal{L}(D)$, er avbildningen også surjektiv. □

Definisjon 1.16. Et *lineært system* $\mathcal{L}$ er et projektivt underrom av det komplette lineære systemet $\mathcal{L}(D)$.

Når vi har etablert at et komplett lineært system har strukturen til et projektivt rom, vil et lineært system utgjøre en mengde hyperplan i det projektive rommet. Hyperplanet assosiert med en divisor D' fra $\mathcal{L}$, kaller vi $H_{D'}$.

$$\begin{aligned}\mathcal{L} =&\{hyperplan\ i\ \mathbb{P}^n\},\\ D' &\longleftrightarrow H_{D'} \subseteq \mathbb{P}^n,\end{aligned}$$

der n er dimensjonen til $\mathcal{L}$ som projektivt rom.

Dersom vi har en kurve C og en divisor D på kurven, vil et lineært system $\mathcal{L} \subseteq \mathcal{L}(D)$ definere en rasjonal avbildning ϕ av kurven inn i et projektivt rom:

$$\begin{aligned}C &\xrightarrow{\phi} \mathbb{P}^n,\\ P &\mapsto \phi(P),\end{aligned}$$

der $\phi(P)$ er et snitt av hyperplan:

$$\phi(P) = \bigcap_{\substack{D'\in\mathcal{L}\\ P\in D'}} H_{D'}.$$

Definisjon 1.17. Dersom et punkt $P \in C$ er i hver divisor i $\mathcal{L}$, kalles P et *basispunkt* for det lineære systemet.

Når hver divisor $D' \in \mathcal{L}$ inneholder P, vil ikke avbildningen ϕ være definert i basispunktet. Hvis $\mathcal{L}$ ikke inneholder noen basispunkter, er ϕ en morfi.

For at snittet av hyperplan skal kunne definere et punkt i $\mathbb{P}^n$, må vi være sikre på at det finnes n ulike hyperplan som inneholder det samme punktet. Et hyperplan er definert av en homogen lineær likning, så n lineært uavhengige slike i $n+1$ variable i $\mathbb{P}^n$ vil gi et éndimensjonalt løsningsrom.

La $D = \sum_{Q\in C} e_Q Q$. En divisor $D' \in \mathcal{L} \subseteq \mathcal{L}(D)$ innholder et punkt P dersom $e'_P = e_P + v_P(f) > 0$. Vi kan definere en mengde $\mathcal{L}_P$ bestående av alle slike divisorer:

$$\mathcal{L}_P = \{D' \in \mathcal{L} | D' \ni P\} = \{D' | e_p + v_p(f) > 0\} \subseteq \mathcal{L} \subseteq \mathcal{L}(D).$$

Vi vil altså finne n effektive divisorer som inneholder punktet P.

La først $P \in C$ være slik at $e_P = 0$ i divisoren D. Siden enhver divisor lineært ekvivalent med D er på formen $D + (f)$ for en $f \in K(C)$, må en divisor ha $v_P(f) > 0$ for at den skal inneholde P. Det betyr at den rasjonale funksjonen er slik at $f(P) = 0$, så f er i det maksimale idealet $m_{C,P}$ i den lokale ringen $\mathcal{O}_{C,P}$. Altså vil alle de rasjonale funksjonene f som har positiv

valuasjon i P, gjøre at $D+(f)$ er en effektiv divisor som inneholder P. Siden $e_P = 0$, vil vektorrommet $\widetilde{\mathcal{L}}$ være inneholdt i $\mathcal{O}_{C,P}$.

La avbildningen ev_P være *evalueringen* av en rasjonal funksjon i P, slik at $ev_P(f) = f(P)$, der $f(P)$ er i restkroppen k_P. Denne avbildningen er surjektiv, slik at vi kan lage en kort eksakt sekvens

$$\begin{aligned} 0 \to m_{C,P} \hookrightarrow & \mathcal{O}_{C,P} \overset{ev_P}{\twoheadrightarrow} k_P \to 0, \\ & f \mapsto f(P). \end{aligned}$$

Ved å restriktere avbildningen ev_P til å kun evaluere funksjonene i $\widetilde{\mathcal{L}}$, får vi sekvensen

$$0 \to \ker\left(ev_P|_{\widetilde{\mathcal{L}}}\right) \hookrightarrow \widetilde{\mathcal{L}} \overset{ev_P|_{\widetilde{\mathcal{L}}}}{\to} k_P \to 0.$$

Dersom det er n rasjonale funksjoner i $\widetilde{\mathcal{L}}$ som blir null når de evalueres i P, har vi funnet n divisorer som inneholder P. Dermed er det dimensjonen til kjernen til $ev_P|_{\widetilde{\mathcal{L}}}$ vi må undersøke:

$$\ker\left(ev_P|_{\widetilde{\mathcal{L}}}\right) = \{f \in \widetilde{\mathcal{L}} \mid f(P) = 0\} = \{f \in \widetilde{\mathcal{L}} \mid v_P(f) > 0\}.$$

Siden dette er mengden rasjonale funksjoner f som gjør at $D+(f)$ inneholder P, kaller vi denne mengden $\widetilde{\mathcal{L}_P}$. Hvis $ev_P|_{\widetilde{\mathcal{L}}}$ er surjektiv, er sekvensen over en kort eksakt sekvens. I så fall har vi et resultat fra [1, kapittel 2] som fastslår at $\dim \widetilde{\mathcal{L}} = \dim \widetilde{\mathcal{L}_P} + \dim k_P$. Siden $\dim k_P = 1$, kan vi i dette tilfellet bestemme dimensjonen til kjernen:

$$\dim\left(\ker\left(ev_P|_{\widetilde{\mathcal{L}}}\right)\right) = \dim \widetilde{\mathcal{L}_P} = \dim \widetilde{\mathcal{L}} - 1.$$

Dersom alle $f \in \widetilde{\mathcal{L}}$ er slik at $f(P) = 0$, er $ev_P|_{\widetilde{\mathcal{L}}}$ ikke surjektiv, men konstant. Da er $\dim \widetilde{\mathcal{L}_P} = \dim \widetilde{\mathcal{L}}$, og P er i så fall et basispunkt i $\mathcal{L}$. Vi skal senere se at vi kan fjerne slike punkter fra det lineære systemet for likevel å kunne definere en morfi ϕ.

Hvis $ev_P|_{\widetilde{\mathcal{L}_P}}$ er surjektiv, får vi altså at nøyaktig n divisorer inneholder punktet P, slik at punktet blir definert av et snitt av hyperplan i $\mathbb{P}^n$.

Anta nå at vi velger et punkt $P \in C$ slik at $e_P \neq 0$ i divisoren D. Vi ønsker nå å finne n divisorer D' i det lineære systemet gitt av D som er slik at koeffisienten $e'_P = e_P + v_P(f)$ er større enn null. For å kunne bruke samme type dimensjonsbetraktning som over, må vi sørge for at alle de rasjonale funksjonene f som gjør at divisoren $D + (f)$ inneholder P, er i kjernen til den restrikterte evalueringen $ev_P|_{\widetilde{\mathcal{L}}}$.

La t generere det maksimale idealet $m_{C,P}$. Da er $v_P(t) = 1$, slik at vi får

$$v_P\left(ft^{e_P}\right) = v_P(f) + e_P v_P(t) = v_P(f) + e_P > -e_P + e_P = 0.$$

Ved å multiplisere hver $f \in \widetilde{\mathcal{L}}$ med t^{e_P}, får vi dermed isomorfien

$$\begin{aligned} \widetilde{\mathcal{L}} &\cong \widetilde{\mathcal{L}} \cdot t^{e_P}, \\ f &\mapsto f t^{e_P}, \end{aligned}$$

der hver f som i $\widetilde{\mathcal{L}}$ er slik at $v_P(f) > -e_P$, i $\widetilde{\mathcal{L}} \cdot t^{e_P}$ blir slik at $v_P(f t^{e_P}) > 0$. Dette gir oss den eksakte sekvensen

$$0 \to \ker\left(ev_P|_{\widetilde{\mathcal{L}}}\right) \hookrightarrow \widetilde{\mathcal{L}} \cdot t^{e_P} \overset{ev_P|_{\widetilde{\mathcal{L}}}}{\to} k_P \to 0,$$

$$\ker\left(ev_P|_{\widetilde{\mathcal{L}}}\right) = \widetilde{\mathcal{L}_P} \cdot t^{e_P}.$$

Dermed kan vi trekke samme konklusjon som når $e_P = 0$ i divisoren D.

Videre vil vi forsikre oss om at vi kan definere en avbildning av kurven inn i projektivt rom selv om $\dim \widetilde{\mathcal{L}_P} = \dim \widetilde{\mathcal{L}}$. I dette tilfellet er P i hver divisor i $\mathcal{L}$, så det er et basispunkt. Vi ønsker å sjekke om det er i orden å fjerne basispunktene fra hver divisor i det linære systemet.

Lemma 1.18. *La $\mathcal{L}$ være et lineært system på en kurve C, og P et basispunkt i $\mathcal{L}$. Trekk P fra hver divisor i $\mathcal{L}$, slik at vi får mengden*

$$\mathcal{L}' = \{D' - P \mid D' \in \mathcal{L}\} \subseteq \mathcal{L}(D - P)$$

Da er $\dim(\mathcal{L}') = \dim(\mathcal{L})$.

Bevis. Når P er et basispunkt, er divisorene $D' - P \geq 0$ for alle $D' \in \mathcal{L}$. Dette betyr at $\dim(\mathcal{L}') = \dim(\mathcal{L})$, slik at de lineære systemene er isomorfe. Når $\mathcal{L}$ definerte en avbildning av kurven inn i $\mathbb{P}^n$, vil dermed også $\mathcal{L}'$ definere en avbildning inn i $\mathbb{P}^n$. Dersom det er flere basispunkter i det lineære systemet, kan vi gjenta denne prosessen. Vi kan være sikre på at ikke *alle* punktene på C er basispunkter, fordi vi i så fall hadde fått en konstantavbildning av kurven til et punkt. □

Med avbildningen gitt av et lineært system av divisorer, kan vi videre se på kurver som kurver i et projektivt plan eller projektivt rom. Divisorer gitt av snitt mellom kurver og hyperplan, divisorklasser og lineære systemer vil videre være nyttige hjelpemidler i beskrivelsen av kurver og spesielle punkter.

Kapittel 2

Riemann-Roch

Det finnes en bestemt sammenheng mellom graden til en divisor D og dimensjonen $l(D)$ til vektorrommet $\widetilde{\mathcal{L}(D)}$. Sammenhengen er gitt av Riemann-Roch-formelen, som vi her skal bruke uten å gi noe bevis (for bevis, se for eksempel [4, kapittel IV.1]). Kurven C har en unik kanonisk divisorklasse (se [6, kapittel II.4]), og vi kaller en divisor fra denne divisorklassen K_C.

Teorem 2.1 (Riemann-Roch)**.** *La C være en kurve, og D en divisor på C. La videre $l(D)$ være* $\dim \widetilde{\mathcal{L}(D)}$*, la g_C være kurvens genus, og K_C en kanonisk divisor på C. Da finnes følgende sammenheng:*

$$l(D) - l(K_C - D) = \deg D + 1 - g_C.$$

Det er flere observasjoner vi kan gjøre ut i fra sammenhengene i Riemann-Roch. Dersom $\deg D < 0$ vil vi ha minst én $e_P < 0$, der $P \in C$. Da er ikke D effektiv, og $\widetilde{\mathcal{L}(D)} = \emptyset$. I dette tilfellet får vi dermed at $l(D) = 0$, så $l(K_C - D) = g_C - 1 - \deg D$. Dersom D er nulldivisoren, vil $\mathcal{L}(D)$ kun inneholde D selv, så dimensjonen til det lineære systemet blir null. Siden $\dim \widetilde{\mathcal{L}(D)} = \dim \mathcal{L}(D)+1$, blir i dette tilfellet vektorromsdimensjonen $l(D) = l(0) = 1$.

La oss undersøke $l(K_C)$. Vi velger først $D = 0$:

$$\begin{aligned} l(0) - l(K_C - 0) &= \deg(0) + 1 - g_C, \\ 1 - l(K_C) &= 1 - g_C, \\ l(K_C) &= g_C. \end{aligned}$$

Vi kan dermed definere kurvens genus som nettopp dimensjonen til vektor-

rommet $\widetilde{\mathcal{L}(K_C)}$. Deretter velger vi $D = K_C$, og får

$$\begin{aligned} l(K_C) - l(K_C - K_C) &= \deg K_C + g_C - 1, \\ g_C - 1 &= \deg K_C - g_C + 2, \\ \deg K_C &= 2g_C - 2. \end{aligned}$$

Om vi her ikke skal se nærmere på den kanoniske divisoren K_C, skal vi i det minste bruke resultatene over.

2.1 Riemann-Roch for $\mathbb{P}^1$

Vi skal nå undersøke hva Riemann-Roch forteller oss om den projektive linjen $\mathbb{P}^1$. Dersom $C = \mathbb{P}^1$ og en divisor på $\mathbb{P}^1$ har grad $d > 0$, vil vektorrommet $\widetilde{\mathcal{L}(D)}$ være isomorft med polynomringen i to variable av grad d. Et vektorrom isomorft med en polynomring i n variable av grad d vil ha dimensjon lik antall mulige monomer av grad d. I dette tilfellet, når $\widetilde{\mathcal{L}(D)} \cong k[x, y]_d$, vil disse monomene være

$$x^d, x^{d-1}y, \ldots, xy^{d-1}, y^d.$$

Dette er $d+1$ monomer, slik at vektorromsdimensjonen, altså $l(D)$, er $d+1$.

Ved å velge d stor nok, altså større enn $\deg(K_{\mathbb{P}^1})$, blir $\deg(K_{\mathbb{P}^1} - D) < 0$. Da får vi

$$\begin{aligned} l(D) - l(K_{\mathbb{P}^1} - D) &= d + 1 - g_{\mathbb{P}^1}, \\ d + 1 - 0 &= d + 1 - g_{\mathbb{P}^1}, \\ g_{\mathbb{P}^1} &= 0. \end{aligned}$$

2.2 Riemann-Roch for elliptiske kurver

En glatt kurve med genus $g = 1$ kalles en *elliptisk kurve*. Riemann-Roch gir oss da følgende for en elliptisk kurve E:

$$\deg K_E = 2g_E - 2 = 2 - 2 = 0,$$

$$l(K_E) = g_E = 1.$$

Av disse to resultatene, kan vi konkludere at K_E er nulldivisoren på E. Videre har vi da:

$$\begin{aligned} l(D) - l(0 - D) &= \deg D + 1 - 1, \\ l(D) - l(-D) &= \deg D. \end{aligned}$$

Hvis $\deg D > 0$, får vi at $l(D) = \deg D$.

Hittil har vi fastslått hva vektorromsdimensjonen til $\widetilde{\mathcal{L}(D)}$ blir dersom graden til D er strengt negativ eller strengt positiv:

$$\begin{aligned} \deg D < 0 &\implies l(D) = 0, \\ \deg D > 0 &\implies l(D) = \deg D. \end{aligned}$$

Hva kan vi si om $l(D)$ dersom $\deg D = 0$? Dersom D er lineært ekvivalent med nulldivisoren, $D \sim 0$, vil $l(D) = 1$. Finnes en divisor D med $\deg D = 0$ og $l(D) = 0$?

Antagelsen $\deg D = 0$ gir oss $\sum_{P' \in E} e_{P'} = 0$. Anta at alle $e'_P = 0$ bortsett fra $e_P = 1$ og $e_Q = -1$, der $P \neq Q$. Da kan vi skrive $D = P - Q$. Vi vil vise at $l(D) = l(P - Q) = 0$, som er ekvivalent med å vise $\widetilde{\mathcal{L}(P - Q)} = \emptyset$. Vi antar derfor at $\widetilde{\mathcal{L}(P - Q)} \neq \emptyset$. Da finnes det en effektiv divisor D' lineært ekvivalent med $P - Q$, slik at $\deg D' = \sum e'_{P'} = 0$. Siden D' er effektiv, er $e'_{P'} \geq 0$ for alle $P' \in E$, så hver $e'_{P'} = 0$. Altså er D' nulldivisoren. Da har vi følgende:

$$\begin{aligned} D' &\sim P - Q, \\ P - Q - D' &= (f), \\ P - Q &= (f), \\ P &\sim Q. \end{aligned}$$

Da er både P og Q i $\mathcal{L}(P)$, så $\dim \mathcal{L}(P) \geq 1$, og $l(P) = \dim \widetilde{\mathcal{L}(P)} \geq 2$. Av Riemann-Roch har vi at $\deg P = 1 = l(P)$, men $1 < 2$, så vi får en selvmotsigelse. Ingen slik D' finnes, så $D \nsim 0$, og vi kan konkludere at $\deg D = 0$ og $l(D) = 0$.

Lemma 2.2. *Hver divisor av grad null er lineært ekvivalent med en divisor på formen $P - Q$, der P og Q er punkter på kurven.*

Bevis. Vi vil finne P og Q slik at $D \sim P - Q$, der D er en hvilken som helst divisor av grad null. Vi velger Q som et hvilket som helst punkt på kurven. Av Riemann-Roch vet vi da at det finnes én effektiv divisor lineært ekvivalent med $D + Q$. Kall denne P. Da er $D \sim P - Q$. □

Vi kan oppsummere det vi vet om vektorromsdimensjonen $l(D)$ i følgende proposisjon:

Proposisjon 2.3.

$$\begin{aligned}
\deg D < 0 &\implies l(D) = 0,\\
\deg D > 0 &\implies l(D) = \deg D,\\
\deg D = 0 &\implies \begin{cases} l(D) = 1 & hvis\ D \sim 0,\\ l(D) = 0 & ellers. \end{cases}
\end{aligned}$$

La oss videre se på to par av punkter på kurven som danner to lineært ekvivalente divisorer, hver av grad null. For fire punkter $P, Q, P', Q' \in E$ har vi:

$$\begin{aligned}
P - Q &\sim P' - Q',\\
(P - Q) - (P' - Q') &= (f),\\
P - Q - P' + Q' &= (f),\\
(P + Q') - (P' + Q) &= (f),\\
P + Q' &\sim P' + Q.
\end{aligned}$$

Av Riemann-Roch er $l(P + Q') = 2$, som betyr at $\dim \mathcal{L}(P + Q') = 1$. Av dette kan vi konkludere at det komplette lineære systemet av alle effektive divisorer lineært ekvivalente med en divisor $P+Q'$, danner en projektiv linje.

Definisjon 2.4. Alle uordnede par av punkter (P, Q), der P og Q er punkter på kurven E (inkludert $P = Q$), utgjør det *symmetriske produktet* $S^2(E)$.

Altså er $S^2(E)$ mengden av alle effektive divisorer av grad 2. Hver projektive linje gitt av et komplett lineært system av grad 2 blir da en ekte undermengde av det symmetriske produktet: $\mathcal{L}(P + Q) \subsetneq S^2(E)$.

Proposisjon 2.5. *Velg et punkt $P \in E$.*

1. *For hvert punkt $Q \in E$ er $\mathcal{L}(P + Q) \subsetneq S^2(E)$.*
2. *Dersom $Q \neq Q'$, er $\mathcal{L}(P + Q)$ disjunkt fra $\mathcal{L}(P + Q')$.*
3. *$S^2(E) = \bigcup_{Q \in E} \mathcal{L}(P + Q)$*

Bevis.

1. Ta en divisor $D \in \mathcal{L}(P + Q)$. Dette er en effektiv divisor av grad 2, så den er i det symmetriske produktet.
2. Anta at $\mathcal{L}(P + Q)$ ikke er disjunkt fra $\mathcal{L}(P + Q')$, altså at de har minst én felles divisor D'. Da vil $D' \sim P + Q$ og $D' \sim P + Q'$, slik at $P + Q \sim P + Q'$. Dermed får vi at $Q = Q'$, som motsier antagelsen vår.
3. Vi mangler $S^2(E) \subseteq \bigcup \mathcal{L}(P+Q)$ for å vise dette. Ta et par av punkter $(P, Q) \in S^2(E)$. Disse to punktene finner vi igjen i $\mathcal{L}(P + Q)$. □

Når vi har fastslått at det symmetriske produktet er en union av disjunkte projektive linjer, kan det være naturlig å spørre hvor mange slike linjer unionen består av.

Lemma 2.6. *Det symmetriske produktet $S^2(E)$ består av like mange projektive linjer som det er punkter på kurven E.*

Bevis. Først kan vi se at unionen må bestå av minst like mange projektive linjer som det er punkter på kurven. Velg et punkt Q, og se på $P+Q$ for alle $P \in E$. Vi har vist at det komplette lineære systemet $\mathcal{L}(P+Q)$ danner en projektiv linje. Hvis $\mathcal{L}(P+Q) = \mathcal{L}(P'+Q)$, har vi følgende:

$$\begin{aligned} P+Q &\sim P'+Q, \\ P &\sim P', \\ P &= P'. \end{aligned}$$

Hvis vi har bestemt et punkt Q, vil altså ulike valg av P gi ulike divisorklasser av grad 2.

Vi kan nå vise at det ikke finnes flere divisorer av grad 2 enn divisorklassene vi har funnet. La D være en divisor med grad 2. Vi vil vise at $D \sim P+Q$ for et punkt $P \in E$. Siden $D-Q$ ikke er effektiv, og $l(D-Q) = 1$, har vi av Riemann-Roch at $D-Q \sim P$ for et punkt P. Da har vi $D \sim P+Q$, som ønsket. □

Mengden av alle divisorklassene på en kurve C utgjør en gruppe kalt *Picard-gruppen* $\mathrm{Pic}(C)$. Alle divisorer i samme divisorklasse har samme grad, og denne graden definerer graden til divisorklassen. En delmengde av $Pic(C)$ bestående av divisorklasser av en bestemt grad d, kalles $Pic_d(C)$. Velg to divisorer D og D' med grad henholdsvis d og d'. Vi får da

$$\begin{aligned} [D] + [D'] &= [D''], \\ D + (f) + D' + (g) = D + D' + (f) + (g) &= D'' + (fg), \end{aligned}$$

der $\deg D'' = d + d'$. Dersom vi legger sammen to divisorklasser av grad null, får vi altså en ny divisorklasse av grad null. Dette skal vi i kapittel 3 bruke til å legge sammen punkter på en elliptisk kurve.

2.3 Elliptiske fjerdegradskurver i $\mathbb{P}^3$

Vi avslutter kapitlet med å undersøke strukturen til en elliptisk kurve i $\mathbb{P}^3$. En romkurve kan være gitt som et snitt av to flater, og vi skal se at et snitt av to annengradsflater, eller *kvadrikker*, i projektivt rom, gir oss en elliptisk

kurve. På den andre siden kan vi vise at en elliptisk kurve i $\mathbb{P}^3$ ligger på to kvadrikker.

La F^2 betegne en kvadrikk. Når en kurve er et *komplett* snitt i $\mathbb{P}^3$, er den definert av nøyaktig to homogene polynomer. Hvert polynom definerer en flate i $\mathbb{P}^3$.

Proposisjon 2.7. *I $\mathbb{P}^3$ er en elliptisk fjerdegradskurve E snittet av to kvadrikker F_1^2 og F_2^2.*

Bevis. Vi forklarer først at et snitt av to kvadrikker er en elliptisk kurve.

I [4, kapittel I.7] kan vi finne at genusen til snittet mellom to flater av grad henholdvis a og b i $\mathbb{P}^3$ gir en kurve av genus $\frac{1}{2}ab(a+b-4)+1$. Hvis begge kurvene har grad 2, blir genusen til snittet dermed lik 1, og i følge teorem 1.9 er snittet en kurve av grad $2 \cdot 2 = 4$. Dette er en elliptisk kurve i $\mathbb{P}^3$.

Videre skal vi vise at en elliptisk kurve $E \subseteq \mathbb{P}^3$ kan uttrykkes som et snitt av to flater gitt av to polynomer av grad 2.

For et punkt $P \in E$, kan vi lage vektorrommet

$$\widetilde{\mathcal{L}(4P)} = \{f \mid (f) + 4P > 0,\ f \in K(E)\}.$$

I følge Riemann-Roch er $\dim \widetilde{\mathcal{L}(4P)} = 4$, så $\dim \mathcal{L}(4P) = 3$, og det lineære systemet definerer dermed en avbildning av kurven inn i $\mathbb{P}^3$. Vi konstruerer basiser for vektorrommene:

$$\begin{aligned}
\widetilde{\mathcal{L}(P)} &= \langle 1 \rangle, \\
\widetilde{\mathcal{L}(2P)} &= \langle 1, x \rangle, \\
\widetilde{\mathcal{L}(3P)} &= \langle 1, x, y \rangle, \\
\widetilde{\mathcal{L}(4P)} &= \langle 1, x, y, x^2 \rangle.
\end{aligned}$$

Her har funksjonene $1, x, y$ og x^2 polorden henholdsvis $1, 2, 3$ og 4. Med et koordinatskifte skriver vi basisen til $\widetilde{\mathcal{L}(4P)}$ som $\langle T_0, T_1, T_2, T_3 \rangle$, og ser at vi får en homogen annengradslikning $T_1^2 = T_3 T_0$. Videre bruker vi funksjonene i basisen til å lage større vektorrom:

$$\begin{aligned}
\widetilde{\mathcal{L}(5P)} &= \langle T_0, T_1, T_2, T_3, T_1T_2 \rangle, \\
\widetilde{\mathcal{L}(6P)} &= \langle T_0, T_1, T_2, T_3, T_1T_2, T_2^2, T_1^3 \rangle, \\
\widetilde{\mathcal{L}(7P)} &= \langle T_0, T_1, T_2, T_3, T_1T_2, T_2^2, T_1^3, T_2T_3 \rangle, \\
\widetilde{\mathcal{L}(8P)} &= \langle T_0, T_1, T_2, T_3, T_1T_2, T_2^2, T_1^3, T_2T_3, T_3^2, T_1T_2^2 \rangle.
\end{aligned}$$

Her har både T_2^2 og T_1^3 polorden 6, og både T_3^2 og $T_1T_2^2$ har polorden 8. Siden $\dim \widetilde{\mathcal{L}(6P)} = 6$, mens basisen til vektorrommet inneholder sju funksjoner, vet vi at det finnes minst én lineærrelasjon mellom dem:

$$a_0T_0 + a_1T_1 + a_2T_2 + a_3T_3 + a_4T_1T_2 + a_5T_2^2 + a_6T_1^3 = 0.$$

Siden basiselementene til $\widetilde{\mathcal{L}(5P)}$ er lineært uavhengige, vet vi at ikke a_5 og a_6 kan være null samtidig. Hvis $a_5 = 0$, men $a_6 \neq 0$, får vi likningen

$$a_0T_0 + a_1T_1 + a_2T_2 + a_3T_3 + a_4T_1T_2 = -a_6T_1^3,$$

der T_1^3 har polorden 6. Summen på venstre side i likningen kan ikke ha høyere polorden enn 5, og kan dermed umulig være lik et uttrykk med polorden 6. Dermed er vi sikre på at verken a_5 eller a_6 er null.

På samme måte får vi lineærrelasjonen mellom basiselementene i $\widetilde{\mathcal{L}(8P)}$:

$$b_0T_0+b_1T_1+b_2T_2+b_3T_3+b_4T_1T_2+b_5T_2^2+b_6T_1^3+b_7T_2T_3+b_8T_3^2+b_9T_1T_2^2 = 0,$$

der verken b_8 eller b_9 er null. Fra basisen til $\widetilde{\mathcal{L}(6P)}$ får vi et uttrykk for T_2^2, og sammen med likheten $T_1^2 = T_3$, får vi

$$T_3^2 = \beta_7T_2T_3 + \beta_6T_1T_3 + \beta_5T_1T_2 + \beta_4T_0T_1 + \beta_3T_3 + \beta_2T_2 + \beta_1T_1 + \beta_0T_0.$$

Ved å homogenisere likningene, får vi de to annengradsflatene i $\mathbb{P}^3$:

1. $T_3^2 = \alpha_6T_2T_3 + \alpha_5T_1T_3 + \alpha_4T_1T_2 + \alpha_3T_0T_3 + \alpha_2T_0T_2 + \alpha_1T_0T_1 + \alpha_0T_0^2$,
2. $T_1^2 = T_0T_3$.

□

Kapittel 3

Gruppestrukturen på elliptiske kurver

Vi spesifiserer en elliptisk kurve til å være kurven sammen med et bestemt valg av origo. Det finnes en gruppestruktur på den elliptiske kurven gitt av dette valget. I dette kapitlet beskrives denne gruppestrukturen både som addisjon av divisorklasser og ved en geometrisk konstruksjon. Til slutt i kapitlet viser vi at tre punkter på en plan elliptisk kurve adderes til null hvis og bare hvis de er kolineære, og tilsvarende at fire punkter på en elliptisk romkurve adderes til null hvis og bare hvis de er koplanare.

3.1 Gruppen $\mathrm{Pic}_0(E)$.

Alle lineært ekvivalente divisorer er inneholdt i samme divisorklasse, og divisorklassene danner en gruppe. Legger vi sammen en divisorklasse av grad m og en av grad n, får vi en divisorklasse av grad $m+n$. Dersom $\deg[D] = \deg[D'] = 0$, vil også $\deg[D+D'] = 0$, så vi får en undergruppe av alle divisorklasser av grad null, kalt $\mathrm{Pic}_0(E)$.

Vi har tidligere sett at enhver divisor av grad null er lineært ekvivalent med en unik divisor på formen $P-Q$. Ved å holde punktet Q fast, vil vi dermed få like mange slike divisorer, og like mange tilhørende divisorklasser, som det er punkter på kurven. Et element $[P-Q]$ i gruppen av divisorklasser av grad null vil unikt representere et punkt P. Dette kan vi bruke til å definere en gruppestruktur på E, og få et nytt punkt ved å addere to punkter. Vi bruker notasjonen $+_{\mathrm{Q}}$ for gruppeoperasjonen når punktet Q er valgt.

Definisjon 3.1. Gruppeaddisjonen av punktene på E er definert på følgende

måte:

$$P +_{\mathrm{Q}} P' = P'' \Rightarrow [P - Q] + [P' - Q] = [P + P' - 2Q] = [P'' - Q]$$

3.2 Geometrisk realisering av gruppestrukturen.

Vi kan få en ekvivalent gruppestruktur ved å definere addisjonen av punktene på kurven med en geometrisk konstruksjon.

En plan elliptisk kurve er gitt av en *Weierstrass-likning* (se [6, kapittel III.1]). Denne er på formen

$$y^2 = x^3 + ax + b, \tag{3.1}$$

der a og b er slik at kurven ikke har noen singulære punkter.

Hvis vi homogeniserer likning (3.1) til $zy^2 = x^3 + az^2x + bz^3$, og setter $z = 0$, får vi $x^3 = 0$, så $x = 0$. Ved Bézouts teorem har vi at en linje vil snitte en kurve av grad d i d punkter, telt med multiplisitet. Siden E har grad 3, og kurven skjærer linja i uendelig i kun ett punkt $(0 : y : 0) = (0 : 1 : 0)$, kan vi konkludere at $(0 : 1 : 0)$ er et vendepunkt, og linja i uendelig en vendetangent til kurven. Videre kaller vi punktet i uendelig for $\mathcal{O}$.

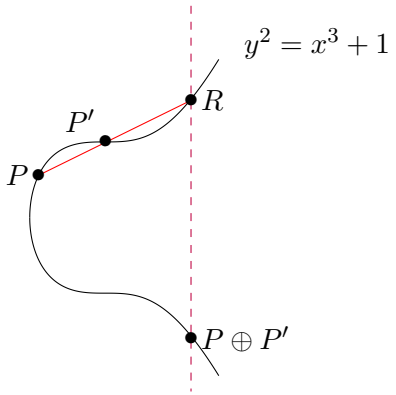
For å beskrive gruppestrukturen, behøver vi en binæroperasjon som virker på disse punktene. Ved å velge et vendepunkt som nøytralt element, får vi den geometriske realiseringen av gruppen som er beskrevet under. Vi velger punktet i uendelig, $\mathcal{O}$, som nøytralt element. Alle linjer parallelle med y-aksen vil skjære i dette punktet.

La E være en elliptisk kurve på formen (3.1). En linje mellom to punkter $P, P' \in E$ vil generelt skjære kurven i et tredje punkt R. Trekker man en linje gjennom R og $\mathcal{O}$, altså en vertikal linje gjennom R på figur 3.1, vil denne linja igjen skjære i et tredje punkt. Dette er punktet som defineres som gruppeaddisjonen av P og P', og vi skriver det som $P \oplus P'$. Denne prosessen er illustrert i figur 3.1.

Vi sjekker at gruppeaksiomene er oppfylt:

Kommutativitet
: Linja mellom P og P' vil skjære kurven i et unikt tredje punkt, så $P \oplus P' = P' \oplus P$.

Identitetselement
: Tegn en linje gjennom $\mathcal{O}$ og P, som snitter kurven i et tredje punkt P'. Ved å følge konstruksjonen over, vil linja mellom $\mathcal{O}$ og P' snitte kurven i P: $P \oplus \mathcal{O} = P = \mathcal{O} \oplus P$.



Figur 3.1: Illustrasjon av addisjon av punkter på en elliptisk kurve.

Invers

Trekk en linje mellom P og $\mathcal{O}$. Linja skjærer kurven i et tredje punkt P'. Da finner vi $P \oplus P'$ ved å se på snittet mellom det tredje snittpunktet, $\mathcal{O}$, og $\mathcal{O}$ selv. Siden $\mathcal{O}$ er et infleksjonspunkt, vil tangentlinjen her ha snittmultiplisitet 3 med kurven, så $P \oplus P' = \mathcal{O}$. Generelt kan vi se at dersom vi trekker en linje mellom to punkter P og P', blir det tredje skjæringspunktet Q inversen til $P \oplus P'$.

Assosiativitet

Å vise at addisjonen er assosiativ, følger ikke like enkelt av konstruksjonen som de andre egenskapene. I kapittel 3.1 så vi at vi kan assosiere hvert punkt på kurven til en divisorklasse av grad null, og bruke at alle disse divisorklassene utgjør en gruppe, til å beskrive en gruppestruktur på E. At addisjonen av divisorklasser av grad null er assosiativ, vil gi at også den geometriske addisjonen beskrevet over er assosiativ.

3.3 Sammenligning av binæroperasjonene

Videre ønsker vi å sjekke at de to addisjonsmetodene gir samme gruppestruktur for samme valg av origo.

Lemma 3.2. *Dersom punktet Q velges til å være punktet i uendelig, $\mathcal{O}$, vil gruppeaddisjonene $+_{\mathcal{O}}$ og $\oplus$ være ekvivalente.*

Bevis. Anta først at vi har gruppeaddisjonen $\oplus$ gitt av den geometriske konstruksjonen beskrevet over, der $P_1 \oplus P_2 = P_3$, og punktet P_4 er det tredje snittpunktet mellom kurven E og linja $l_{P_1P_2}$. Da har vi følgende:

$$E \cap l_{P_1P_2} = \{P_1, P_2, P_4\},$$
$$E \cap l_{P_4\mathcal{O}} = \{\mathcal{O}, P_4, P_3\}.$$

De to divisorene $P_1 + P_2 + P_4$ og $\mathcal{O} + P_4 + P_3$ er da i det lineære systemet $\{\text{div}_E(E \cap l)\}$, så de er lineært ekvivalente. For en $f \in K(E)$, har vi da:

$$\begin{aligned} P_1 + P_2 + P_4 &\sim \mathcal{O} + P_4 + P_3, \\ P_1 + P_2 + P_4 - \mathcal{O} - P_4 - P_3 &= (f), \\ P_1 + P_2 - \mathcal{O} - P_3 &= (f), \\ P_1 + P_2 + \mathcal{O} &\sim P_3, \\ P_1 + P_2 - 2\mathcal{O} &\sim P_3 - \mathcal{O}. \end{aligned}$$

Da vil divisorklassene $[P_1 + P_2 - 2\mathcal{O}]$ og $[P_3 - \mathcal{O}]$ være like, slik at vi får

$$\begin{aligned} [P_1 + P_2 - 2\mathcal{O}] &= [P_3 - \mathcal{O}], \\ [P_1 - \mathcal{O}] + [P_2 - \mathcal{O}] &= [P_3 - \mathcal{O}], \end{aligned}$$

som betyr at $P_1 +_{\mathcal{O}} P_2 = P_3$.

Anta nå at vi har addisjonen av divisorklasser av grad null, og tre punkter P_1, P_2, P_3 som er slik at $P_1 +_{\mathcal{O}} P_2 = P_3$. Da har vi følgende:

$$\begin{aligned} [P_1 - \mathcal{O}] + [P_2 - \mathcal{O}] &= [P_3 - \mathcal{O}], \\ [P_1 + P_2 - 2\mathcal{O}] &= [P_3 - \mathcal{O}], \\ P_1 + P_2 - 2\mathcal{O} &\sim P_3 - \mathcal{O}, \\ P_1 + P_2 &\sim P_3 + \mathcal{O}. \end{aligned}$$

La P_4 betegne det tredje snittpunktet mellom kurven og linja $l_{P_1P_2}$. Da har vi den lineære ekvivalensen $P_1 + P_2 + P_4 \sim P_3 + \mathcal{O} + P_4$, slik at linja gjennom P_3 og $\mathcal{O}$ også skjærer kurven i P_4. I den geometriske konstruksjonen av gruppeaddisjonen på punktene på E er da P_4 og P_3 inverser, slik at $P_1 \oplus P_2 = P_3$. □

Videre bruker vi kun notasjonen $\oplus$ for addisjonen i gruppa av punkter på en elliptisk kurve E.

Proposisjon 3.3. *$P_1 \oplus P_2 \oplus P_3 = \mathcal{O} \iff P_1, P_2$ og P_3 er kolineære*

Merk at dette gjelder generelt for $P_1 \oplus P_2 \oplus P_3 = P_0$, så lenge P_0 er et infleksjonspunkt.

Bevis. Anta først at $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$. Konstruksjonen av denne binæroperasjonen gir oss

$$\begin{aligned} [P_1 - \mathcal{O}] + [P_2 - \mathcal{O}] + [P_3 - \mathcal{O}] &= [0], \\ [P_1 + P_2 + P_3 - 3\mathcal{O}] &= [0], \\ P_1 + P_2 + P_3 - 3\mathcal{O} &\sim 0, \\ P_1 + P_2 + P_3 &\sim 3\mathcal{O}. \end{aligned}$$

Siden graden til kurven E er 3, vil $3\mathcal{O}$ være divisoren gitt av snittet mellom tangentlinja $T_{\mathcal{O}}(E)$ og E. Da er $3\mathcal{O}$ i det komplette lineære systemet $\{\text{div}_E(E \cap l)\}$ gitt av snittene mellom kurven og linjer l. I dette lineære systemet finner vi da også $P_1 + P_2 + P_3$, slik at denne divisoren også er gitt av snittet mellom kurven og en linje.

Anta nå at P_1, P_2 og P_3 ligger på linje. Konstruksjonen av binæroperasjonen gir oss $(P_1 \oplus P_2) \oplus P_3 = \mathcal{O}$. □

La nå $E \subseteq \mathbb{P}^3$ være en elliptisk kurve med grad 4 og genus 1. Et plan vil generelt skjære kurven i fire punkter.

Proposisjon 3.4. *La E være en elliptisk kurve i $\mathbb{P}^3$ med et punkt P_0 slik at et plan snitter E med multiplisitet 4 i P_0. Velg P_0 til å være origo i gruppa av punkter på kurven. Da blir summen av fire punkter på kurven P_0 hvis og bare hvis de er koplanare.*

Bevis. Vi vil altså vise ekvivalensen

$$P_1 \oplus P_2 \oplus P_3 \oplus P_4 = P_0 \iff \{P_1, P_2, P_3, P_4\} = E \cap \pi' \text{ for et plan } \pi'.$$

Anta først at fire punkter P_1, P_2, P_3, $P_4 \in E$ er slik at $P_1 \oplus P_2 \oplus P_3 \oplus P_4 = P_0$. Gruppeaddisjonen på punktene på E gir oss da:

$$\begin{aligned} P_1 \oplus P_2 \oplus P_3 \oplus P_4 &= P_0, \\ [P_1 - P_0] + [P_2 - P_0] + [P_3 - P_0] + [P_4 - P_0] &= [0], \\ [P_1 + P_2 + P_3 + P_4 - 4P_0] &= [0], \\ P_1 + P_2 + P_3 + P_4 - 4P_0 &\sim 0, \\ P_1 + P_2 + P_3 + P_4 &\sim 4P_0. \end{aligned}$$

Punktet P_0 er slik at divisoren $4P_0 = \text{div}_E\, E \cap H_{P_0}$, der H_{P_0} er et plan, som betyr at $4P_0$ er i det komplette lineære systemet $\{\text{div}_E(E \cap \pi\}$ gitt av snitt mellom E og plan π. Da er også $P_1 + P_2 + P_3 + P_4$ i dette lineære systemet, så det finnes et plan alle de fire punktene ligger i.

Anta nå at de fire punktene er koplanare. Da er divisoren $P_1 + P_2 + P_3 + P_4$ i det komplette lineære systemet $\{\text{div}_E(E \cap \pi\}$. Her finner vi også $4P_0$, slik at $P_1 + P_2 + P_3 + P_4 \sim 4P_0$. Da er $P_1 \oplus P_2 \oplus P_3 \oplus P_4 = P_0$. □

Merk at vi i proposisjon 3.4 tar for gitt at et punkt P_0 som beskrevet eksisterer. Vi skal i kapittel 5 vise at dette faktisk er tilfellet.

Kapittel 4

Infleksjonspunkter på en kurve i $\mathbb{P}^2$

Videre skal se vi på avbildninger fra en kurve i $\mathbb{P}^2$ som skal brukes til å telle opp infleksjonspunktene på kurven. For å gjøre dette behøver vi et viktig resultat som sier noe om sammenhengen mellom visse egenskaper til to kurver man har definert en avbildning mellom. Dette resultatet er *Hurwitz' formel*, og er hentet fra [4, kapittel IV.2].

4.1 Hurwitz' formel

La $f : X \longrightarrow Y$ være en avbildning mellom to kurver. Her vil antall punkter i fiberen over et punkt på Y være graden n til f, og e_P er koeffisientene i fiberdivisoren. Vi har da *Hurwitz' formel*:

$$2g_X - 2 = n(2g_Y - 2) + \sum_{P \in X} (e_P - 1). \tag{4.1}$$

Eksempel 4.1. La E være en elliptisk kurve, og D en divisor på E av grad 2. Da vil $\dim \mathcal{L}(D) = 1$, slik at vi får definert en avbildning $\phi : E \longrightarrow \mathbb{P}^1$. Siden $\deg D = 2$ vil fibrene til ϕ består av to punkter telt med multiplisitet, så graden til ϕ er 2. Vi vil nå bruke Hurwitz' formel til å finne antall divisorer på formen $2P$ som er lineært ekvivalent med D.

$$2g_E - 2 = \deg\phi(2g_{\mathbb{P}^1} - 2) + \sum_{P\in E}(e_P - 1),$$
$$2\cdot 1 - 2 = 2(2\cdot 0 - 2) + \sum_{P\in E}(e_P - 1),$$
$$\sum_{P\in E}(e_P - 1) = 4.$$

Siden vi skal finne antall divisorer som er på formen $2P$, setter vi $e_P = 2$ og får

$$\sum_{P\in E}(e_P - 1) = \sum_{P\in E}(2 - 1) = \sum_{P\in E} 1 = 4.$$

Av dette kan vi konkludere at det finnes fire divisorer på formen $2P$ lineært ekvivalent med en gitt divisor av grad 2.

4.2 Antall infleksjonspunkter

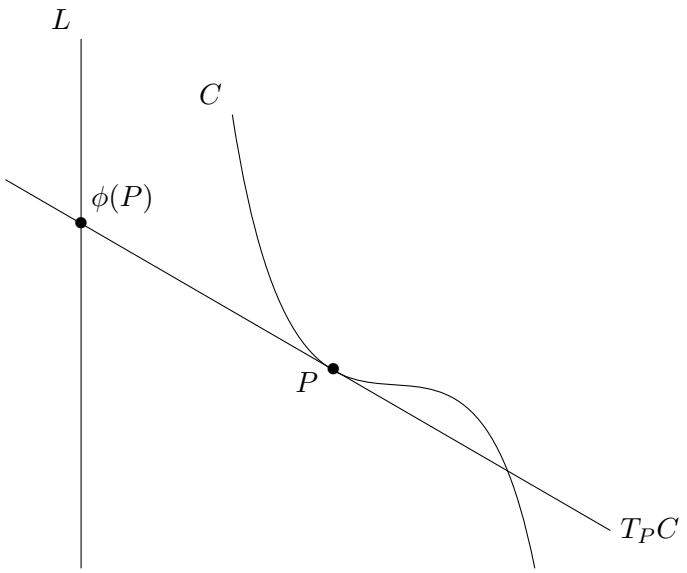
La C være en generell glatt kurve av grad d i $\mathbb{P}^2$. En generell kurve har endelig mange vendepunkter, og alle vendetangenter har snittmultiplisitet 3 med C. I tillegg vil endelig mange tangentlinjer tangere kurven i mer enn ett punkt. La $T_P(C)$ være den entydige tangentlinja til C i punktet P. Vi kan lage følgende avbildning fra kurven til en linje (se figur 4.1):

$$\phi : C \longrightarrow L,$$
$$P \mapsto \phi(P) = T_P(C) \cap L.$$

Merk at linja L ikke kan være en tangent til C: Dersom $L = T_{P'}(C),\ P' \in C$, vil ϕ sende P' på hele L.

Videre har vi at fiberen $\phi^{-1}(q)$, der q er et punkt på L, vil inneholde alle punkter på C som har tangentlinje som skjærer L i q. Vi kan beskrive punktene i fiberen ved hjelp av *ramifikasjonen* til avbildningen.

Definisjon 4.2 (Ramifikasjon)**.** Gitt en morfi av kurver $\psi : C \longrightarrow C'$. For et punkt $Q \in C'$ vil fiberen være en mengde punkter $\psi^{-1}(Q) = \{P_1, \ldots, P_r\}$. Fiberdivisoren er definert som $\psi^*(Q) = e_{P_1}P_1 + \ldots + e_{P_r}P_r$, der ramifikasjonskoeffisienten $e_{P_i} = 1$ for alle unntatt endelig mange $P_i \in \psi^{-1}(Q)$. I tillegg defineres graden til morfien som $\deg\psi = \sum_{i=1}^{r} e_{P_i}$. Merk at $\deg\psi$ er uavhengig av Q. Punktet P_n er et *ramifikasjonspunkt for* ψ dersom $e_{P_n} > 1$, og *ramifikasjonen* til ψ er definert som $R_\psi = \sum_{P\in C}(e_P - 1)$.



Figur 4.1: Illustrasjon av ϕ.

Vi definerer også en projeksjon $\pi_q : C \longrightarrow L'$ fra et projeksjonssenter $q \in L$ til en linje L':

$$\begin{aligned} \pi_q : C &\longrightarrow L', \\ P &\mapsto l_{qP} \cap L'. \end{aligned}$$

Graden til π_q er d, siden fiberen, mengden av punktene i snittet mellom C og en linje gjennom q, består av d punkter. Siden kurven er generell, vil en linje fra et generelt punkt på L *verken* være en vendetangent for kurven *eller* tangere kurven i flere punkter enn ett.

Heretter vil ramifikasjonskoeffisientene for de ulike avbildningene skilles ved å skrive e^{ϕ} og e^{π_q}.

Lemma 4.3. *Punktet P er et ramifikasjonspunkt for π_q hvis og bare hvis linja mellom q og P, l_{Pq}, tangerer C i P.*

Bevis. Fiberen til π_q består av d punkter, og siden vi ser på et generelt punkt q og en generell kurve C, vil fiberdivisoren være på formen

$$\pi_q^* = \operatorname{div}_C(l_{Pq} \cap C) = \begin{cases} \sum_{i=1}^{d} P_i & \text{dersom } l_{Pq} \text{ ikke tangerer } C, \\ 2P + \sum_{j=3}^{d} P_j & \text{dersom } l_{Pq} \text{ tangerer } C \text{ i } P. \end{cases}$$

Ramifikasjonen til π_q er $R_{\pi_q} = \sum(e_{P_i}^{\pi_q} - 1)$, så kun punktene med koeffisient 2 i π_q^* vil gi bidrag. Mengden av ramifikasjonspunkter blir dermed alle punkter

P slik at linja mellom P og q er lik $T_P(C)$, altså mengden

$$\{P \mid 2P + \sum_{j=3}^{d} P_j \in \pi_q^*\}. \qquad \square$$

Korollar 4.4. $R_{\pi_q} = d(d-1)$.

Bevis. Av Hurwitz' formel, se kapittel 4.1, får vi likningen

$$\begin{aligned} 2g_C - 2 &= \deg \pi_q(2g_{L'} - 2) + R_{\pi_q}, \\ R_{\pi_q} &= 2(g_C - 1) + 2d, \end{aligned}$$

siden $g_{L'} = 0$. Siden C er en glatt kurve, vil $g_C = \frac{1}{2}(d-1)(d-2)$ (se for eksempel [4, kapittel I.7]). Dermed har vi:

$$\begin{aligned} R_{\pi_q} &= 2(g_C - 1) + 2d, \\ &= (d-1)(d-2) - 2 + 2d, \\ &= d^2 - 3d + 2 - 2 + 2d = d(d-1). \end{aligned} \qquad \square$$

Lemma 4.5. *Et punkt $P \in C$ er et ramifikasjonspunkt for ϕ hvis og bare hvis det er et infleksjonspunkt eller er slik at $P \in C \cap L$.*

Bevis. For avbildningen ϕ har vi fiberen over et generelt punkt $q \in L$:

$$\begin{aligned} \phi^{-1}(q) &= \{P \in C \mid T_P(C) \cap L = q\}, \\ &= \{P \in C \mid 2P + \sum_{i=3}^{d} P_i = \operatorname{div}_C(l_{Pq} \cap C)\}. \end{aligned}$$

I tillegg har vi fiberdivisoren $\phi^*(q) = \sum_{P \in C} e_P^\phi P$, der $e_P^\phi = 1$ unntatt for endelig mange punkter P, og $\deg \phi = \sum_{P \in C} e_P^\phi$.

Ved å sammenligne fiberen til ϕ over q og ramifikasjonspunktene til π_q, får vi sammenhengen

$$\sum_{P \in C} e_P^\phi = \sum_{P \in C} (e_P^{\pi_q} - 1).$$

Altså er graden til ϕ lik ramifikasjonsgraden til π_q.

Hvis $q \notin C$, vil et snitt mellom C og en linje l_q fra q, gi en divisor på en av følgende former:

$$\begin{aligned} P_1 + \cdots + P_d &= \textstyle\sum_{i=1}^{d} P_i, \\ 2P + P_3 + \cdots + P_d &= \textstyle\sum_{i=3}^{d} P_i + 2P, \\ 3P + P_4 + \cdots + P_d &= \textstyle\sum_{i=4}^{d} P_i + 3P, \\ 2P_1 + 2P_2 + P_5 + \cdots + P_d &= \textstyle\sum_{i=5}^{d} P_i + 2P_1 + 2P_2. \end{aligned}$$

Mengden av disse divisorene vil utgjøre et lineært system $\{\mathrm{div}_C(l_q \cap C)\}$. Kun punktene som har koeffisient større enn 2 i divisorene, vil gi bidrag i ramifikasjonen $R_\phi = \sum_{P \in C}(e_P^\phi - 1)$. Derfor vil infleksjonspunktene på kurven være ramifikasjonspunkter for ϕ.

Hvis projeksjonssenteret q er et punkt på C, vil q være med i alle divisorene gitt av et snitt mellom en linje fra q og C. Disse divisorene vil være på en av følgende former:

$$\begin{gathered} q + P_2 + \cdots + P_d, \\ 2q + P_3 + \cdots + P_d, \\ q + 2P + P_4 + \cdots + P_d. \end{gathered}$$

Her er q et basispunkt i det lineære systemet av disse divisorene. En projeksjon fra q vil dermed ikke definere noen avbildning, og vi kan derfor ikke bruke Hurwitz' formel. Heldigvis viste vi i lemma 1.18 at vi trygt kan trekke fra basispunktet fra hver divisor, og fortsatt ha et like stort lineært system. Divisorene vil da være på en av følgende former:

$$\begin{gathered} P_2 + \cdots + P_d, \\ 2P + P_4 + \cdots + P_d, \\ q + P_3 + \cdots + P_d. \end{gathered}$$

Når $q \in C$, vil $\deg \pi_q = d-1$, så Hurwitz' gir oss at $R'_{\pi_q} = 2(g_C - 1) + 2d - 2$, som er $(d-2)(d+1)$ dersom C er glatt. Graden til avbildningen ϕ fant vi til å være $\deg \phi = 2(g_C - 1) + 2d$. Generelt får vi nå fiberdivisoren

$$\phi^*(q) = \underbrace{P_1 + \cdots + P_n}_{2(g_C-1)+2d-2} + \sum_i e_{P_i} P_i. \tag{4.2}$$

Siden R'_{π_q} er 2 mindre enn $\deg \phi$, er eneste mulighet for en generell C og et generelt punkt $q \in L \cap C$ å ha $\sum e_P = 2$. Et punkt $P \neq q$ er med i summen (4.2) hvis og bare hvis $T_P(C) \cap L = q$, og divisorkoeffisienten til P blir da 1. I summen (4.2) er de n første punktene slike punkter. Det eneste mulige gjenværende punktet å ha med i fiberen er q selv, og vi vet at dette punktet da må ha divisorkoeffisient 2. Dermed er q et ramifikasjonspunkt for ϕ. □

Teorem 4.6. *En glatt, plan kurve C med grad d har $3d(d-2)$ infleksjonspunkter.*

Bevis. Ved å bruke Hurwitz' med $\deg \phi = 2(g_C - 1) + 2d$, får vi $R_\phi = 6(g_C - 1) + 4d$. Ved å trekke fra de d punktene i $C \cap L$, får vi $6(g_C - 1) + 3d$

infleksjonspunkter. Siden C er glatt og $g_C = \frac{1}{2}(d-1)(d-2)$, får vi

$$\begin{aligned} R_\phi &= 6(g_C - 1) + 3d \\ &= 3(d-1)(d-2) - 6 + 3d \\ &= 3d^2 - 9d + 6 - 6 + 3d \\ &= 3d(d-2). \end{aligned}$$

□

Korollar 4.7. *En elliptisk kurve $E \subseteq \mathbb{P}^2$ har ni infleksjonspunkter*

Bevis. En elliptisk kurve $E \subseteq \mathbb{P}^2$ gitt av en Weierstrass-likning har grad 3. Da har E $3 \cdot 3(3-2) = 9$ infleksjonspunkter. □

Definisjon 4.8 (Torsjonspunkter på en elliptisk kurve)**.** La P være et punkt på en elliptisk kurve E, og $P_0 \in E$ origo i gruppa av punkter på kurven. Dersom $nP = P_0$, der $nP = \overbrace{P \oplus \cdots \oplus P}^{n}$, sier vi at P er et *n-torsjonspunkt.*

La $P \in E$ være et av de ni infleksjonspunktene. Da vil snittet mellom $T_P(E)$ og E i P ha multiplisitet 3, slik at vi av proposisjon 3.3 får $P \oplus P \oplus P = 3P = P_0$ for et valgt origo P_0. Punktet P er derfor et 3-*torsjonspunkt.*

Vi ønsker videre å gjennomføre samme type argumentasjon som over for å finne antall punkter tilsvarende infleksjonspunkter på en kurve i $\mathbb{P}^3$.

Kapittel 5

Hyperoskulerende punkter på en kurve i $\mathbb{P}^3$

Et plan som snitter en kurve i rommet med multiplisitet 3 kalles et *oskulerende plan*. Dersom snittmultiplisiteten mellom et plan og kurven er minst 4 i et punkt, kalles planet og punktet *hyperoskulerende*. På en kurve i $\mathbb{P}^n$ vil de hyperoskulerende punktene være der snittmultiplisiteten er minst $n+1$. På en kurve i $\mathbb{P}^2$ er dette infleksjonspunktene. I dette kapitlet skal vi telle opp de hyperoskulerende punktene på en kurve i $\mathbb{P}^3$.

La $C \subseteq \mathbb{P}^3$ være en generell kurve som utspenner $\mathbb{P}^3$. Da er C glatt, og snittmultiplisiteten mellom et hyperoskulerende plan og kurven er nøyaktig 4. La L være en linje som ikke snitter C.

For å kunne definere en avbildning ϕ fra kurven til linja på en tilsvarende måte som i kapittel 4.2, må vi være sikre på at vi for hvert punkt $P \in C$ kan finne et unikt oskulerende plan H_P. Kun et endelig antall punkter på kurven vil være hyperoskulerende. Vi kaller antall hyperoskulerende punkter på en kurve i $\mathbb{P}^n$ for $\mathrm{hyp_n}$, slik at $\mathrm{hyp_2} = 6(g_C - 1) + 3d$.

For et gitt punkt $P \in C$, kan vi lage mengden Ω av alle plan π som inneholder tangentlinja $T_P(C)$:

$$\Omega = \{\pi \mid T_P(C) \subset \pi\}.$$

Snittet mellom hvert plan π i Ω og kurven gir oss et lineært system

$$\{\mathrm{div}_C(\pi \cap C) \mid T_P(C) \subset \pi\}.$$

Siden et plan $\pi \in \Omega$ og C har minst dobbel kontakt i P, vil en divisor i dette lineære systemet være på formen $2P + P_1 + \cdots + P_r$. Ved å trekke fra $2P$ fra hver divisor, får vi et nytt lineært system, med divisorer på formen $D_k = P_1 + \cdots + P_r$. For hvert punkt $P_i \in C$ må det finnes en k slik at

$P_i \in D_k$. Da må det også finnes en k' slik at $P \in D_{k'}$. Siden vi allerede har trukket fra $2P$, må divisoren vi i dette tilfellet startet med være på formen $3P + P_1 + \cdots + P_s$. Planet som snittet med kurven gir denne divisoren, har snittmultiplisitet minst 3 med C i P. For å få en entydig avbildning fra kurven til linja, må vi være sikre på at det ikke finnes flere plan av denne typen for et gitt punkt $P \in C$.

Lemma 5.1. *La P være et punkt på kurven C. Dersom det finnes et plan som har snittmultiplisitet 2 med C i P, kan vi finne et unikt oskulerende plan i P.*

Bevis. Snittmultiplisiteten mellom et av planene $\pi \in \Omega$ og kurven vil være minst 2. Anta at minst to av disse planene har snittmultiplisitet minst 3 med kurven, slik at det finnes minst to oskulerende plan. Se på det lineære systemet $\mathcal{L}(D_k)$ for D_k som over. Det tilsvarende vektorrommet er

$$\widetilde{\mathcal{L}(D_k)} = \{f \mid D_k + (f) > 0\} = \{f \mid v_{P_i}(f) \geq -e_{P_i}\}.$$

Dette vektorrommet har dimensjon 2, og har basis $\{f_1, f_2\}$. Siden vi kan finne minst to divisorer som fortsatt inneholder P, har vi at $v_P(f_1) \geq -e_P + 1$ og $v_P(f_2) \geq -e_P + 1$, slik at $v_P(\lambda f_1 + \mu f_2) \geq -e_P + 1$ for vilkårlige konstanter λ, μ. Altså vil $v_P(f) \geq -e_P + 1$ for alle $f \in \widetilde{\mathcal{L}(D_t)}$, så alle planene $\pi \in \Omega$ har minst trippel kontakt med kurven i P. Dersom vi holder fast ved at det skal finnes et plan som har snittmultiplisitet 2 med kurven i P, kan det altså ikke finnes minst to plan som har snittmultiplisitet minst 3. Dermed finnes kun ett oskulerende plan i et punkt $P \in C$. □

Avbildningen ϕ skal sende et punkt $P \in C$ til snittpunktet mellom det oskulerende planet H_P og linja L. Siden vi er i projektivt rom, er vi sikre på at snittet ikke er tomt. Et problem oppstår derimot dersom L ligger i et plan H_P, siden P da ikke vil bli sendt til noe bestemt punkt. Vi ønsker derfor å spesifisere linja til å ikke ligge i noe oskulerende plan. Vi undersøker om det er mulig å finne en slik linje:

Dersom vi har et endelig antall plan i rommet, kan vi velge et punkt som ikke ligger i noen av disse. Tar vi da hvilken som helst av linjene som går gjennom dette punktet, har vi funnet en linje som ikke ligger i noen av planene. Vi har et oskulerende plan for hvert punkt på kurven, og har derfor uendelig mange plan. Kan vi likevel finne en linje som ikke ligger i noen av disse? Antar vi at vi velger et punkt q utenfor kurven som ligger i uendelig mange H_P, må punktet da ligge i *alle* de oskulerende planene. Vi kan finne et punkt som ikke ligger på alle de oskulerende planene ved å unngå ett av dem.

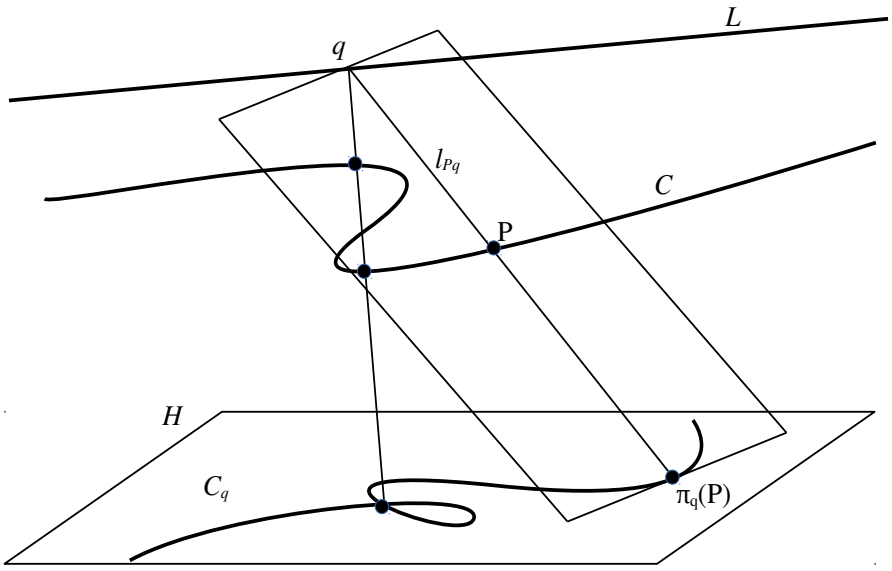
Derfor vil vi kunne finne et punkt $Q_1 \notin C$ som ligger i et endelig antall oskulerende plan. Velger vi nå et annet punkt Q_2 som ikke ligger i noen av

disse endelig mange planene, vil linja $l_{Q_1Q_2}$ oppfylle kravene vi har satt på L, så $L = l_{Q_1Q_2}$. Vi har dermed avbildningen klar:

$$\begin{aligned} \phi : C &\longrightarrow L, \\ P &\mapsto \phi(P) = H_P \cap L. \end{aligned}$$

I $\mathbb{P}^3$ vil avbildningen π_q projisere C via $q \in L$ til en kurve $C_q = \pi_q(C)$ i et projektivt plan H. Linja l_{Pq} er gitt av en fast $q \in L$ og et punkt $P \in C$. Snittet mellom l_{Pq} og H gir et punkt $P' \in C_q$.

$$\begin{aligned} \pi_q : C &\longrightarrow C_q \subseteq H, \\ P &\mapsto \pi_q(P) = l_{Pq} \cap H. \end{aligned}$$



Figur 5.1: Illustrasjon av projeksjonen via $q \in L$ av en kurve C i $\mathbb{P}^3$ til en kurve C_q i planet H. Punktet $P \in C$ blir projisert til punktet $\pi_q(P) \in C_q$.

Utifra denne projeksjonen kan vi lage en avbildning som definerer linjer i H: Planet definert av $T_P(C)$ og projeksjonssenteret q vil snitte H i en linje (se figur 5.1). Snittmultiplisiteten mellom planet og kurven i rommet vil være lik snittmultiplisiteten mellom linja og kurven i det projektive planet, så generelt vil linja tangere C_q:

$$I_P\left(C, T_P(C)\right) = I_{P'}\left(C_q, T_{P'}(C_q)\right).$$

Dersom planet gitt av $T_P(C)$ og q er oskulerende, vil snittmultiplisiteten mellom $T_{P'}(C_q)$ og C_q være 3 i P'. I så fall er P' et infleksjonspunkt. Graden til ϕ er lik antall punkter på kurven som har oskulerende plan som skjærer L i et gitt punkt q. Vi kan dermed trekke følgende konklusjon:

Lemma 5.2. *Antall hyperoskulerende punkter på C_q vil være lik antall oskulerende plan til C som skjærer L i q, som igjen vil være graden til ϕ. I $\mathbb{P}^3$ vil vi dermed ha* $\deg \phi = \text{hyp}_2 = 6(g_C - 1) + 3d$.

Dersom $l_{P_1 q} = l_{P_2 q}$ for to ulike punkter $P_1, P_2 \in C$, vil $\pi_q(P_1) = \pi_q(P_2) = P'$ være en node på C_q. En linje som skjærer kurven i to punkter kalles en sekant, og vi kan alltid finne sekanter for en projeksjon π_q. Dermed kan vi konkludere at den projiserte kurven C_q er singulær. Projeksjonen fra et generelt punkt på L vil gi en nodal kurve i planet. Fra et endelig antall projeksjonssentere $q \in L$ blir C_q cuspidal. Hvis $l_{Pq} = T_P(C)$ får vi nemlig en hel familie av plan gitt av $T_P(C)$ og q, så punktet $\pi_q(P) = P'$ er en cusp på C_q.

Vi skal se at de hyperoskulerende punktene vil gi bidrag til ramifikasjonen R_ϕ. Ved å finne ut av hvilke andre punkter som gir bidrag til R_ϕ, vil vi kunne finne tallet hyp_3.

Lemma 5.3. *Ramifikasjonen til $\phi : C \longrightarrow L$, $\phi(P) = H_P \cap L$, er $R_\phi =$* $\text{hyp}_3 + d_3$, *der* hyp_3 *er antall hyperoskulerende punkter på kurven, og d_3 er antall punkter som har tangentlinje som snitter L.*

Bevis. For et punkt $q \in L$ vil fiberen $\phi^{-1}(q)$ bestå av punkter på C som har oskulerende plan som skjærer L i q. Dersom vi lar q være projeksjonssenteret til π_q, vil punktene i $\phi^{-1}(q)$ projiseres til infleksjonspunkterpunkter på C_q. Fiberdivisoren er da gitt som

$$\phi^*(q) = \sum_{\substack{P \in C \\ \pi_q(P)\ inf}} e_P^\phi P.$$

Summen er altså tatt over punktene på C som projiseres til infleksjonspunkter på C_q. For punktene i fiberdivisoren som er oskulerende, er divisorkoeffisienten 1. Dersom det finnes et punkt P_1 i fiberen som er hyperoskulerende, vil vi få $e_{P_1}^\phi = 2$. Ramifikasjonskoeffisienten blir da $e_{P_1}^\phi - 1 = 2 - 1 = 1$, så hvert hyperoskulerende punkt gir bidrag 1 til ramifikasjonen R_ϕ.

La nå $P_2 \in C$ være slik at $l_{P_2 q} = T_{P_2}(C)$, slik at C_q er en cuspidal kurve av grad d og geometrisk genus $g_{C_q} = g_C$. Ved å følge fremgangsmåten i beviset til teorem 4.6, finner vi at C_q har $6(g_C - 1) + 3d - 1$ infleksjonspunkter. Siden graden $\deg \phi = 6(g_C - 1) + 3d$ er konstant, må $e_{P_2}^\phi = 2$. Dermed vil bidraget til ramifikasjonen R_ϕ fra et slikt punkt P_2 være $e_{P_2}^\phi - 1 = 2 - 1 = 1$.

Siden C er generell, vil ingen andre punkter enn disse to typene gi bidrag til ramifikasjonen til ϕ. □

Hurwitz' gir oss nå:

$$2(g_C - 1) = -2\text{hyp}_2 + \text{hyp}_3 + d_3. \tag{5.1}$$

For å finne d_3 kan vi undersøke unionen av alle tangentlinjene til C. Disse utgjør en flate kalt *tangentdevelopabelen* τ:

$$\tau = \bigcup_{P \in C} T_P(C).$$

Antall punkter i snittet mellom tangentdevelopabelen og linja L vil være d_3. Dette tallet er lik graden til tangentdevelopabelen, som er gitt av kurvens grad og genus. Følgende formel for $\deg \tau$ er hentet fra [5]:

$$d_3 = \deg \tau = 2(g_C - 1) + 2d.$$

Vi finner dermed antall hyperoskulerende punkter på en generell kurve i $\mathbb{P}^3$:

Teorem 5.4. *På en generell kurve C i $\mathbb{P}^3$ med genus g_C og grad d, er antallet hyperoskulerende punkter*

$$\text{hyp}_3 = 12(g_C - 1) + 4d.$$

Bevis. Med uttrykket for d_3 blir likning 5.1

$$\begin{aligned} 2(g_C - 1) &= -2(6(g_C - 1) + 3d) + \text{hyp}_3 + 2(g_C - 1) + 2d, \\ \text{hyp}_3 &= 12(g_C - 1) + 4d. \end{aligned}$$

□

Proposisjon 5.5. *En elliptisk fjerdegradskurve $E \subseteq \mathbb{P}^3$ har 16 hyperoskulerende punkter.*

Bevis. La en elliptisk kurve E i $\mathbb{P}^3$ ha grad $d = 4$ og genus $g_E = 1$. Av teorem 5.4 får vi da:

$$\text{hyp}_3 = 12(g_C - 1) + 4d = 4 \cdot 4 = 16.$$

□

I proposisjon 3.4 var det altså et krav om at origo P_0 måtte velges som et hyperoskulerende punkt. Med et slikt valg vil fire punkter på kurven adderes til P_0 hvis og bare hvis de ligger i samme plan. Siden vi finner et plan som snitter E firedobbelt i et hyperoskulerende punkt P, vil vi få $P \oplus P \oplus P \oplus P = 4P = P_0$. Dermed kan vi konkludere at P er et 4-torsjonspunkt. Vi skal senere se at noen av de 16 hyperoskulerende punktene på E faktisk er 2-torsjonspunkter.

Korollar 5.6. *Det finnes ikke flere 4-torsjonspunkter på $E \subseteq \mathbb{P}^3$ enn de hyperoskulerende punktene.*

Bevis. La $P \in E$ være et 4-torsjonspunkt, slik at $4P = P_0$. Av proposisjon 3.4 vet vi det finnes et plan som snitter E kun i punktet P. Dette planet er dermed hyperoskulerende, så P er et hyperoskulerende punkt. □

Kapittel 6

4-torsjonspunkter på en elliptisk kurve i $\mathbb{P}^3$

Vi har funnet ut at det er 16 hyperoskulerende punkter på en elliptisk kurve i $\mathbb{P}^3$. Kall mengden av disse punktene H_4:

$$H_4 = \{P \in E \mid 4P = E \cap H_P,\ for\ et\ plan\ H_P\}.$$

Siden E er av grad 4, gir Bézout (se teorem 1.9) at et plan vil snitte kurven i fire punkter, telt med multiplisitet. En fjerdegradsflate vil generelt snitte kurven i 16 punkter.

Lemma 6.1. *Snittpunktet mellom E og et plan utspent av tre punkter i H_4, vil også være i H_4.*

Bevis. Velg $P_1, P_2 \in H_4$. Da vil de to divisorene $4P_1$ og $4P_2$ være lineært ekvivalente. Dersom et punkt $P \in E$ er slik at $4P \sim 4P_1$, er også P et hyperoskulerende punkt. Velg nå et tredje punkt $P_3 \in H_4$, slik at $4P_2 \sim 4P_1$ og $4P_3 \sim 4P_1$. La π være planet utspent av P_1, P_2 og P_3, slik at $\pi \cap E = \{P_1, P_2, P_3, P\}$, der P er et fjerde punkt på E. Vi får da, for $f_1, f_2, f_3 \in K(E)$:

$$\begin{aligned} P + P_1 + P_2 + P_3 &\sim 4P_1, \\ P + P_1 + P_2 + P_3 - 4P_1 &= (f_1), \\ 4P + 4P_1 + 4P_2 + 4P_3 - 16P_1 &= (f_2). \end{aligned}$$

Ved å videre bruke at $4P_2 \sim 4P_1$ og $4P_3 \sim 4P_1$, får vi

$$\begin{aligned} 4P + 4P_1 + 4P_2 - 4P_1 + 4P_3 - 4P_1 - 8P_1 &= (f_2), \\ 4P + 4P_1 - 8P_1 &= (f_3). \end{aligned}$$

Dette betyr at $4P - 4P_1 = (f_3)$, så $4P \sim 4P_1$. □

Lemma 6.2. *Mengden av hyperoskulerende punkter på $E \subseteq \mathbb{P}^3$ er en abelsk gruppe av orden* 16*.*

Bevis. H_4 er en delmengde av gruppa av alle punktene på E. Da mangler vi å vise at H_4 er lukket under gruppeaddisjonen, som vi tidligere har vist at er kommutativ. Ta tre punkter $P_0,\ P_1,\ P_2 \in H_4$, der P_0 er origo på E. Av lemma 6.1 har vi at et plan gjennom tre punkter i H_4 vil snitte E i et fjerde punkt som også er hyperoskulerende. Samtidig har vi proposisjon 3.4, som sier at fire punkter ligger i samme plan hvis og bare hvis de adderes til null. La et plan være utspent av P_0, P_1 og P_2, og kall det fjerde snittpunktet med E for P'. Da vil $P_0 \oplus P_1 \oplus P_2 \oplus P' = P_0$. Kall videre summen av P_1 og P_2 for P_3, slik at vi får:

$$\begin{aligned} P_1 \oplus P_2 &= P_3, \\ [P_1 - P_0] + [P_2 - P_0] &= [P_3 - P_0], \\ P_1 - P_0 + P_2 - P_0 &\sim P_3 - P_0, \\ P_1 + P_2 &\sim P_3 + P_0, \\ P_1 + P_2 - P_3 - P_0 &= (f),\ f \in K(E). \end{aligned}$$

Vi kan legge til og trekke fra $P_0 + P'$ på venstre side i likheten, og få ekvivalensen

$$P_1 + P_2 + P_0 + P' \sim P_3 + 2P_0 + P'.$$

Siden det finnes et plan som snitter E i P_1, P_2, P_0 og P', vil denne lineære ekvivalensen gi oss at det også finnes et plan som skjærer E i P', P_3 og med snittmultiplisitet 2 i P_0. Siden P_0 og P' er i H_4, er også P_3 i H_4. □

Proposisjon 6.3. 16 *punkter på E adderes til null hvis og bare hvis de ligger på en fjerdegradsflate F^4.*

Bevis. Vi ønsker altså å vise følgende:

$$\begin{gathered} P_1 \oplus \cdots \oplus P_{16} = \sum_{\substack{i=1 \\ \oplus}}^{i=16} P_i = P_0 \\ \Updownarrow \\ \{P_1, \ldots, P_{16}\} = E \cap F^4. \end{gathered}$$

Anta først at de 16 punktene adderes til null, der addisjonen er binæroperasjonen i gruppa av punktene på E.

$$\begin{aligned} P_1 \oplus \cdots \oplus P_{16} &= P_0, \\ [P_1 + \cdots + P_{16} - 16P_0] &= [0], \\ P_1 + \cdots + P_{16} &\sim 16P_0. \end{aligned}$$

Siden $4P_0$ er en divisor gitt av snittet mellom det hyperoskulerende planet H_{P_0} og kurven, vil divisoren $16P_0$ være inneholdt i det lineære systemet $\{\mathrm{div}_E(E \cap \pi_1 \cdot \pi_2 \cdot \pi_3 \cdot \pi_4)\}$ gitt av snittet mellom kurven og en fjerdegradsflate bestående av fire plan. Dette lineære systemet er komplett, og siden vi har den lineære ekvivalensen $\sum_{i=1}^{16} P_i \sim 16P_0$, er også de 16 punktene i fire plan.

Anta nå at de 16 punktene ligger på en fjerdegradsflate F^4. Da er divisoren gitt av snittet mellom F^4 og E inneholdt i det komplette lineære systemet $\{\mathrm{div}_E(E \cap F_1^4)\}$ gitt av snitt mellom E og enhver fjerdegradsflate. I dette komplette lineære systemet finner vi også divisoren $P_1' + \cdots + P_{16}'$ gitt av snittet mellom E og fire plan π_1, π_2, π_3 og π_4. Da har vi den lineære ekvivalensen

$$P_1 + \cdots + P_{16} \sim P_1' + \cdots + P_{16}',$$

som gir likheten

$$\sum_{\substack{i=1 \\ \oplus}}^{16} P_i = \sum_{\substack{i=1 \\ \oplus}}^{16} P_i'.$$

Siden $P_1', \ldots, P_{16}'$ er 16 punkter der fire og fire er koplanare, er summen av disse

$$\sum_{\substack{i=1 \\ \oplus}}^{16} P_i' = \sum_{\substack{j=1 \\ \oplus}}^{4} P_{0j} = P_0.$$

Derfor blir $P_1 \oplus \cdots \oplus P_{16} = P_0$. □

Kapittel 7

Sammenhengen mellom $\mathbb{Z}_4 \times \mathbb{Z}_4$ og H_4

Vi vil i dette kapitlet vise isomorfien mellom H_4 og $\mathbb{Z}_4 \times \mathbb{Z}_4$. Med denne sammenhengen kan vi videre bruke elementene i $\mathbb{Z}_4 \times \mathbb{Z}_4$ for å si noe om de hyperoskulerende punktene på en elliptisk fjerdegradskurve i $\mathbb{P}^3$.

Gruppa $\mathbb{Z}_4 \times \mathbb{Z}_4$ inneholder 16 elementer på formen (a, b), der $a, b \in \{0, 1, 2, 3\}$. Vi kaller antall elementer i en gruppe for gruppas *orden*, og skriver $|\mathbb{Z}_4 \times \mathbb{Z}_4| = 16$. Vi ønsker å finne alle undergruppene av orden 4. En slik undergruppe vil enten være isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_2$ eller $\mathbb{Z}_4$.

$$\mathbb{Z}_4 = \{0, 1, 2, 3\},$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

Undergruppa $\mathbb{Z}_4$ er generert av både 1 og 3, så $\mathbb{Z}_4$ er *syklisk*. Ingen av elementene i $\mathbb{Z}_2 \times \mathbb{Z}_2$ generer hele gruppa, så den er *ikke* syklisk. Ved å sjekke om en undergruppe til $\mathbb{Z}_4 \times \mathbb{Z}_4$ av orden 4 er syklisk, finner vi ut om den er isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_2$ eller $\mathbb{Z}_4$.

Definisjon 7.1. La a være et element i en gruppe med identitetselement e. *Ordenen* til a er det minste tallet m slik at $ma = e$. Vi skriver $\text{ord}(a) = m$.

I $\mathbb{Z}_4 \times \mathbb{Z}_4$ kan vi sjekke ordenen til hvert enkelt element. De mulige ordenene er 1, 2 og 4, siden ordenen til et element i en gruppe må dele ordenen til gruppa (se for eksempel [3, kapittel II.10]), og i tillegg vil vi ikke finne elementer av orden $8 = 2 \cdot 4$ eller $16 = 4 \cdot 4$. Identitetselementet $(0, 0)$ har orden 1. Det finnes 12 elementer som har orden 4, der to elementer som er inverse genererer samme undergruppe av $\mathbb{Z}_4 \times \mathbb{Z}_4$. De siste tre elementene, $(0, 2)$, $(2, 0)$ og $(2, 2)$, har orden 2, og utgjør, sammen med identiteten, undergruppen som ikke er syklisk. Vi har dermed telt opp sju undergrupper av orden 4:

1. $\{(0,0),(0,1),(0,3),(0,2)\}$.
2. $\{(0,0),(2,1),(2,3),(0,2)\}$.
3. $\{(0,0),(1,0),(3,0),(2,0)\}$.
4. $\{(0,0),(1,2),(3,2),(2,0)\}$.
5. $\{(0,0),(1,1),(3,3),(2,2)\}$.
6. $\{(0,0),(3,1),(1,3),(2,2)\}$.
7. $\{(0,0),(2,2),(2,0),(0,2)\}$.

Proposisjon 7.2. *Gruppa H_4 av hyperoskulerende punkter på en elliptisk romkurve er isomorf med $\mathbb{Z}_4 \times \mathbb{Z}_4$.*

Bevis. De abelske gruppene av orden 16 er $\mathbb{Z}_{16}$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ og $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Alle de hyperoskulerende punktene er slik at $4P = P_0$ for et valgt origo $P_0 \in H_4$. Da er den maksimale ordenen til elementene i H_4 4, noe som utelukker en isomorfi med $\mathbb{Z}_{16}$ og $\mathbb{Z}_2 \times \mathbb{Z}_8$.

Dersom et hyperoskulerende punkt er slik at $2P = P_0$, vil det være et 2-torsjonspunkt og ha orden 2. I kapittel 10 vil vi i lemma 10.2 vise at tre av de hyperoskulerende punktene er av orden 2. Punktet som velges som origo har orden 1. Derfor er H_4 verken isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, som har elementer med orden høyest 2, eller med $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, som har sju elementer av orden 2 og 8 elementer av orden 4. Heldigvis har den siste abelske gruppen av orden 16, $\mathbb{Z}_4 \times \mathbb{Z}_4$, like mange elementer av de ulike ordenene som H_4. □

Korollar 7.3. *De* 16 4*-torsjonspunktene på E ligger på en fjerdegradsflate.*

Bevis. Legger man sammen alle elementene i $\mathbb{Z}_4 \times \mathbb{Z}_4$ får man det nøytrale elementet $(0,0)$, altså null i gruppa. Ved å bruke isomorfien mellom punktene i H_4 og elementene i $\mathbb{Z}_4 \times \mathbb{Z}_4$ i proposisjon 7.2, vet vi at alle elementene i H_4 også summeres til null. Ved å bruke proposisjon 6.3, kan vi konkludere at de 16 4-torsjonspunktene på E ligger på en fjerdegradsflate. □

Vi ønsker å dele de 16 elementene inn i fire delmengder, der hver delmengde inneholder fire elementer som lagt sammen blir null. Geometrisk har vi da funnet fire plan som tilsammen snitter E i alle de 16 hyperoskulerende punktene. De fire planene danner et *tetraeder*, og vi kan undersøke hvor mange slike tetraedere vi kan finne på en elliptisk kurve i $\mathbb{P}^3$. Først skal vi se på den tilsvarende problemstillingen for en elliptisk kurve E i $\mathbb{P}^2$, der vi ser på linjer gjennom tre og tre infleksjonspunkter. Har man tre linjer som tilsammen skjærer alle de ni infleksjonspunktene, danner disse en trekant i $\mathbb{P}^2$.

Kapittel 8

Antall trekanter gjennom infleksjonspunktene på E i $\mathbb{P}^2$

Vi har tidligere funnet ut at en elliptisk kurve $E \subseteq \mathbb{P}^2$ har $3d(d-2) = 3 \cdot 3 = 9$ infleksjonspunkter. Mengden av disse punktene utgjør en undergruppe av E som vi kaller H_3. Vi ønsker i dette kapitlet å vise følgende proposisjon:

Proposisjon 8.1. *Det finnes fire trekanter gjennom de ni infleksjonspunktene på en elliptisk kurve i* $\mathbb{P}^2$*.*

For å vise dette, fastslår vi først isomorfien $H_4 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Proposisjon 8.2. *Gruppa* H_3 *av infleksjonskurver på en plan elliptisk kurve er isomorf med* $\mathbb{Z}_3 \times \mathbb{Z}_3$*.*

Bevis. Vi vet at $|H_3| = |\mathbb{Z}_3 \times \mathbb{Z}_3| = 9$. Alle infleksjonspunktene $P_i \in H_3$ er slik at $3P_i = P_0$ for et valgt origo $P_0 \in H_3$. Derfor har alle infleksjonspunktene orden maksimalt 3. Origo vil ha orden 1. Siden ordenen til hvert element må dele ordenen til gruppa, vil ingen elementer i H_3 ha orden 2. Vi sjekker isomorfien ved å undersøke ordenen til elementene i $\mathbb{Z}_3 \times \mathbb{Z}_3$:

$$\mathbb{Z}_3 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (2,0), (1,1), (2,2), (1,2), (2,1)\}.$$

I gruppa er $\text{ord}((0,0)) = 1$ mens ordenen til de resterende åtte elementene er 3. □

I proposisjon 3.3 viste vi at tre punkter på E ligger på linje hvis og bare hvis summen av dem blir null. Vi ønsker å finne antall tripler av linjer som tilsammen skjærer E i alle infleksjonspunktene. Proposisjon 8.2 gir oss at vi kan tilegne hvert punkt i H_3 et element i $\mathbb{Z}_3 \times \mathbb{Z}_3$, for så å se på en inndeling av disse elementene i tre nullsummer. Summen som inneholder $(0,0)$ må

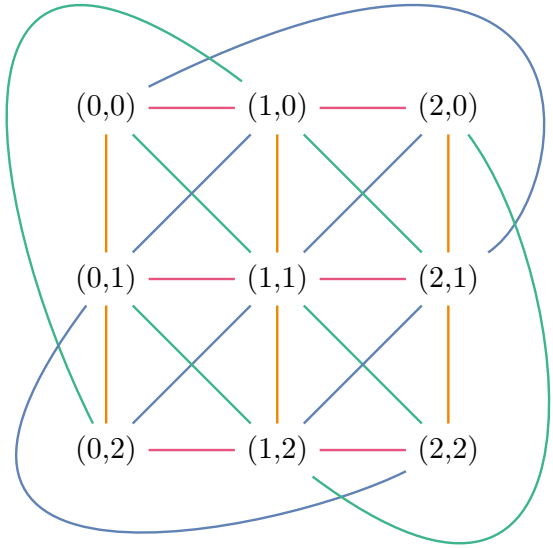
forøvrig bestå av et inverspar, så vi har fire muligheter for denne summen. For hvert valg av inverspar, finnes bare én mulighet for de to andre summene.

Eksempel 8.3. Vi velger inversparet $(1,0),(2,0)$ til første sum, blir de ni elementene delt i tre summer som dette:

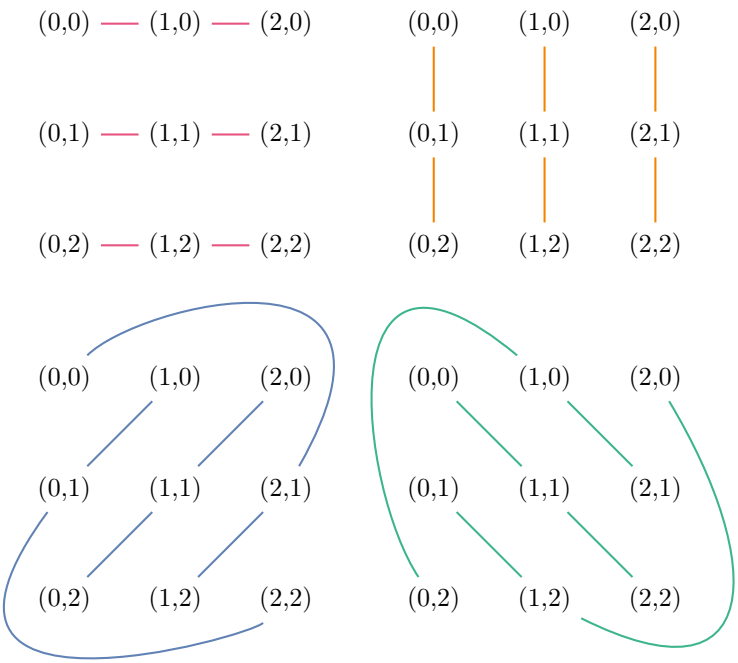
$$(0,0)+(1,0)+(2,0)=(0,0),$$
$$(0,1)+(2,1)+(1,1)=(0,0),$$
$$(0,2)+(1,2)+(2,2)=(0,0).$$

Tilsammen har vi funnet $3\cdot 4 = 12$ linjer gjennom tre og tre infleksjonspunkter på E. Disse 12 linjene kan deles i fire trekanter som skjærer kurven i alle punktene i H_3. Vi har dermed vist proposisjon 8.1.

De fire trekantene er illustrert i figur 8.1, og de er illustert hver for seg i figur 8.2. Merk at siden kurven er i det projektive planet over de komplekse tallene, kan vi ikke illustrere triplene av linjer som reelle trekanter.



Figur 8.1: De ni infleksjonspunktene på $E \subseteq \mathbb{P}^2$ gitt som elementene i $\mathbb{Z}_3 \times \mathbb{Z}_3$. En trekant som skjærer E i alle infleksjonspunktene, er på figuren illustrert som tre linjer i samme farge.



Figur 8.2: Her er de fire trekantene gjennom infleksjonspunktene på E i hver sin figur.

Kapittel 9

Antall tetraedere gjennom de hyperoskulerende punktene på E i $\mathbb{P}^3$

I dette kapitlet skal vi vise følgende teorem:

Teorem 9.1. *Det finnes 713 tetraedere gjennom de 16 hyperoskulerende punktene på en elliptisk fjerdegradskurve i* $\mathbb{P}^3$.

Hvert av de fire planene i et tetraeder skal inneholde fire punkter fra H_4. Antall tetraedere blir da antall måter følgende ligningssett er oppfylt, med $P_i \in H_4$, $0 \leq i \leq 15$, der P_0 er valgt som origo:

$$\begin{aligned} P_0 + P_1 + P_2 + P_3 &= P_0, \\ P_4 + P_5 + P_6 + P_7 &= P_0, \\ P_8 + P_9 + P_{10} + P_{11} &= P_0, \\ P_{12} + P_{13} + P_{14} + P_{15} &= P_0. \end{aligned}$$

Tidligere har vi vist at $H_4 \cong \mathbb{Z}_4 \times \mathbb{Z}_4$. Vi vil derfor assosiere hvert hyperoskulerende punkt P_i, $0 \leq i \leq 15$, med et element (m, n), $m, n \in \{0, 1, 2, 3\}$, i $\mathbb{Z}_4 \times \mathbb{Z}_4$. Da kan vi løse det geometriske problemet kun ved hjelp av det vi vet om elementene i gruppa.

Lemma 9.2. *La* 12 *av elementene i* $\mathbb{Z}_4 \times \mathbb{Z}_4$ *være fordelt i tre summer, der hver sum har fire ledd, og hver sum er null. Da vil summen av de siste fire elementene også være null.*

Bevis. Summen av alle elementene i $\mathbb{Z}_4 \times \mathbb{Z}_4$ blir null. Trekker man fra de 12 elementene beskrevet i lemmaet, har vi trukket fra null. Summen av de fire elementene som er igjen, vil da også være null. □

9.1 Første fordeling

I den abelske gruppa $\mathbb{Z}_4 \times \mathbb{Z}_4$ finner vi ett element av orden 1, tre elementer av orden 2 og 12 elementer av orden 4. Vi bruker dette til å finne ulike fordelinger, og starter med fire summer strukturert etter orden som dette:

$$\begin{array}{cccc} 1 & 2 & 2 & 2 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{array}$$

I rad to har vi 12 elementer av orden 4 å velge mellom, og vi skal velge fire slik at summen av dem blir null. De 12 elementene er:

$$\begin{array}{cc} (1,0)\ (3,0) & (1,2)\ (3,2) \\ (0,1)\ (0,3) & (2,1)\ (2,3) \\ (1,3)\ (3,1) & (1,1)\ (3,3) \end{array}$$

Kall mengden av disse elementene A, slik at et element a er i A hvis og bare hvis $\text{ord}(a) = 4$. Et element i A vil generere en undergruppe av $\mathbb{Z}_4 \times \mathbb{Z}_4$, og inversen til dette elementet vil generere samme undergruppe. For eksempel har vi $\langle(1,0)\rangle = \langle(3,0)\rangle = \{(1,0),(2,0),(3,0),(0,0)\}$. Altså, hvis $a = -a'$, der $a,\ a' \in A$, så vil $2a = 2a' = b$, der $\text{ord}(b) = 2$.

Lemma 9.3. *La to ulike elementer $a,\ b \in A$ være slik at $2a = 2b$ og $a \neq -b$. Da genererer de to elementene en undergruppe av $\mathbb{Z}_4 \times \mathbb{Z}_4$ av orden 8. Det finnes tre slike undergrupper. Legger man sammen to orden 4-elementer fra to ulike undergrupper, får man et element av orden 4 som er i den tredje ungergruppa.*

Bevis. Vi har følgende undergrupper av orden 4:

$$\begin{aligned} \langle(1,0)\rangle &= \langle(3,0)\rangle = \{(1,0),(2,0),(3,0),(0,0)\}, \\ \langle(1,2)\rangle &= \langle(3,2)\rangle = \{(1,2),(2,0),(3,2),(0,0)\}, \\ \langle(0,1)\rangle &= \langle(0,3)\rangle = \{(0,1),(0,2),(0,3),(0,0)\}, \\ \langle(2,1)\rangle &= \langle(2,3)\rangle = \{(2,1),(0,2),(2,3),(0,0)\}, \\ \langle(1,3)\rangle &= \langle(3,1)\rangle = \{(1,3),(2,2),(3,1),(0,0)\}, \\ \langle(1,1)\rangle &= \langle(3,3)\rangle = \{(1,1),(2,2),(3,3),(0,0)\}. \end{aligned}$$

Her kan vi se at $(1,0)$, $(3,0)$, $(1,2)$ og $(3,2)$ alle genererer elementet $(2,0)$. Vi finner undergruppa generert av to av disse elementene:

$$\langle(1,0),(1,2)\rangle = \{(0,0),(1,0),(1,2),(2,2),(3,2),(3,0),(2,0),(0,2)\}.$$

Man kan sjekke at $\langle(1,0),(1,2)\rangle = \langle(1,0),(3,2)\rangle = \langle(3,0),(1,2)\rangle$. Videre finner vi de to andre undergruppene:

$$\langle(0,1),(2,1)\rangle = \{(0,0),(0,1),(2,1),(0,2),(0,3),(2,2),(2,3),(2,0)\}.$$

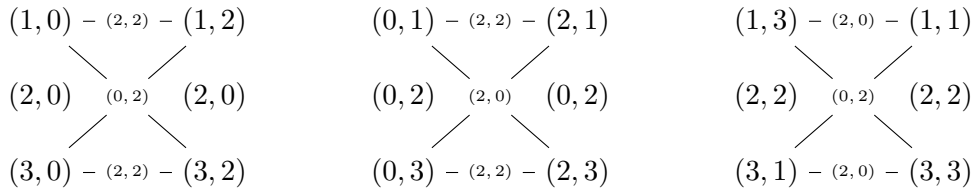
$$\langle(1,1),(1,3)\rangle = \{(0,0),(1,1),(1,3),(2,2),(3,3),(2,0),(3,1),(0,2)\}.$$

Vi legger sammen to elementer av orden 4 fra to ulike undergrupper:

$$\begin{aligned}(1,0)+(0,1)&=(1,1),\\(1,0)+(2,1)&=(3,1),\\(1,0)+(0,3)&=(1,3),\\(1,0)+(2,3)&=(3,3).\end{aligned}$$

Her får vi kun elementer fra den tredje undergruppen. Det er mulig å sjekke videre at dette alltid gjelder. □

Vi illustrerer de nevnte undergruppene av orden 4 og orden 8.



Figur 9.1: Hver av de seks kolonnene inneholder et inverspar og 2-torsjonselementet i undergruppa av orden 4. Summen av to og to elementer er markert.

Lemma 9.4. *Anta $a+b+c+d=(0,0)$ for ulike elementer $a,b,c,d\in A$. Da er $a+b+c+d$ på en av følgende former:*

a) $a+b=c+d=(0,0)$, *og* $\operatorname{ord}(a+c)=\operatorname{ord}(a+d)=\operatorname{ord}(b+c)=\operatorname{ord}(b+d)=2$. *Det finnes tre slike 4-tupler. Vi bruker betegnelsen* $(0,2,2)$ *for å henvise til et 4-tuppel av denne typen.*

b) $a+b=c+d=(0,0)$, *og* $\operatorname{ord}(a+c)=\operatorname{ord}(a+d)=\operatorname{ord}(b+c)=\operatorname{ord}(b+d)=4$. *Det finnes* 12 *slike 4-tupler. Vi bruker betegnelsen* (0) *for å henvise til et 4-tuppel av denne typen.*

c) $a+b=c+d$, $\operatorname{ord}(a+b)=\operatorname{ord}(c+d)=2$, *og* $\operatorname{ord}(a+c)=\operatorname{ord}(a+d)=\operatorname{ord}(b+c)=\operatorname{ord}(b+d)=4$. *Det finnes* 12 *slike 4-tupler. Vi bruker betegnelsen* (2) *for å henvise til et 4-tuppel av denne typen.*

Bevis.

a) I et 4-tuppel av denne typen vil alle elementene være fra samme undergruppe av orden 8. Det finnes tre slike undergrupper, og dermed tre summer av denne typen.

b) I et 4-tuppel av denne typen velger man to inverspar fra to ulike undergrupper av orden 8. Et valg av to slike undergrupper gir fire 4-tupler. Siden vi kan velge to undergrupper på tre ulike måter, får vi $3 \cdot 4 = 12$ summer av denne typen.

c) I et 4-tuppel av denne typen skal to og to elementer lagt sammen bli det samme elementet av orden 2. I figur 9.1 er denne typen summer av to elementer illustrert. For hvert valg av to elementer i summen, må de to andre velges fra én annen undergruppe av orden 8, siden vi ikke kan få et element av orden 2 ved å legge sammen to elementer fra ulike undergrupper. Velger vi to undergrupper å telle fra, finner vi fire 4-tupler på den ønskede formen. Siden vi har tre måter å velge to undergrupper, får vi $3 \cdot 4 = 12$ summer av denne typen.

Når vi skal velge fire elementer av orden 4, må minst to av dem være i samme undergruppe av orden 8. Da vil alltid minst to av elementene i en sum $a+b+c+d$ være inverser av hverandre eller summeres til et element av orden 2. Siden vi kun ser på 4-tupler som summeres til null, og summen av to elementer fra to ulike undergrupper alltid blir et element av orden 4, vil elementene i summen $a+b+c+d = (0,0)$ alltid måtte velges fra maksimalt to undergrupper av orden 8. Alle mulige kombinasjoner av fire elementer fra én eller to slike undergrupper, der summen av elementene er null, er på én av de tre formene i lemmaet. □

Eksempel 9.5.

a) $(1,0)+(3,0)+(1,2)+(3,2)$ er en av de tre mulige radene av type $(0,2,2)$ siden summen består av to inverspar, og $\text{ord}((1,0)+(1,2)) = \text{ord}((3,0)+(3,2)) = 2$.

b) $(1,0)+(3,0)+(0,1)+(0,3)$ er en av de 12 mulige radene av type (0) siden summen består av to inverspar, og $\text{ord}((1,0)+(0,1)) = \text{ord}((1,0)+(0,3)) = \text{ord}((3,0)+(0,1)) = \text{ord}((3,0)+(0,3)) = 4$.

c) $(1,0)+(3,2)+(1,3)+(3,3)$ er en av de 12 mulige radene av type (2) siden $(1,0)+(3,2) = (0,2) = (1,3)+(3,3)$, og $\text{ord}((1,0)+(1,3)) = \text{ord}((1,0)+(3,3)) = \text{ord}((3,2)+(1,3)) = \text{ord}((3,2)+(3,3)) = 4$.

Vi skal sette sammen tre 4-tupler slik at hver av de tre summene blir null. Formen til de tre summene vil bli beskrevet ved hjelp av notasjonen fra lemma 9.4. For eksempel vil tre $(0,2,2)$-rader skrives $(0,2,2)^3$. Vi undersøker følgende muligheter for de tre radene:

1) $(0,2,2)^3$.

2) $(0,2,2)(0)^2$.

3) $(0,2,2)(2)^2$.

4) $(0)^3$.

5) $(0,2,2)(0)(2)$.

6) $(2)^3$.

7) $(2)^2(0)$.

8) $(2)(0)^2$.

9) $(0,2,2)^2(0)$.

10) $(0,2,2)^2(2)$.

Dersom to av de tre radene velges på formen $(0,2,2)$, vil de siste fire elementene også utgjøre en rad på denne formen. Derfor vil vi ikke finne noen fordelinger av typene 9) og 10). Dersom to rader velges på formen (2), vil de siste fire elementene utgjøre en $(0,2,2)$-rad, så vi kan ikke finne fordelinger av typene 6) og 7). Dersom to av radene er på formen (0), vil den siste enten være en (0)- eller $(0,2,2)$-rad. Derfor kan vi ikke finne noen fordelinger av type 8). Dersom to av radene velges til å være av typene $(0,2,2)$ og (0), vil den siste raden også bestå av to inverspar. Dette kan ikke være en (2)-rad, så vi vil heller ikke finne noen fordelinger på form 5). Vi står igjen med fire typer sammensetninger av radene: $(0,2,2)^3$, $(0,2,2)(0)^2$, $(0,2,2)(2)^2$ og $(0)^3$. Videre ønsker vi å finne ut av hvor mange muligheter hver type vil gi.

1) Av figur 9.1 og lemma 9.4 *a*) ser vi at vi kan finne én sammensetning av de 12 elementene i A på formen $(0,2,2)^3$. De tre summene blir:

$$\begin{aligned}(1,0)+(3,0)+(1,2)+(3,2)&=(0,0),\\(0,1)+(0,3)+(2,1)+(2,3)&=(0,0),\\(1,3)+(3,1)+(1,1)+(3,3)&=(0,0).\end{aligned}$$

2) Vi har tre $(0,2,2)$-rader å velge mellom til sammensetningen $(0,2,2)(0)^2$. For hvert valg av en rad av denne typen, står vi igjen med fire (0)-rader som kan velges til de siste to radene. Velger vi for eksempel $(1,0)+(3,0)+(1,2)+(3,2)$ som $(0,2,2)$-rad, har vi følgende muligheter for de to neste:

$$\begin{aligned}(0,1)+(0,3)+(1,3)+(3,1),\\(0,1)+(0,3)+(1,1)+(3,3),\\(2,1)+(2,3)+(1,3)+(3,1),\\(2,1)+(2,3)+(1,1)+(3,3).\end{aligned}$$

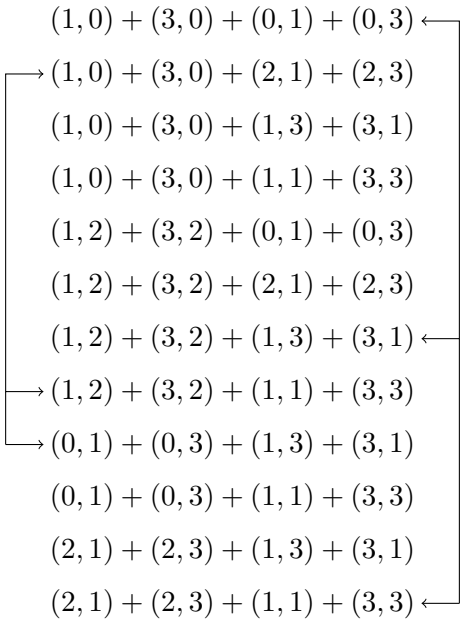
Av disse summene kan vi telle opp to ulike mulige fordelinger av alle elementene. Tilsammen har vi da $3\cdot 2=6$ strukturer på denne formen.

3) For sammensetningen $(0,2,2)(2)^2$ har vi igjen tre $(0,2,2)$-rader å velge mellom. Velges for eksempel $(1,0)+(3,0)+(1,2)+(3,2)$, har vi følgende (2)-rader å velge mellom:

$$(0,1)+(2,3)+(1,3)+(1,1),$$
$$(0,1)+(2,3)+(3,1)+(3,3),$$
$$(2,1)+(0,3)+(1,3)+(1,1),$$
$$(2,1)+(0,3)+(3,1)+(3,3).$$

Dette gir oss to ulike måter å strukturere de siste åtte elementene på, slik at vi tilsammen får $3 \cdot 2 = 6$ muligheter.

4) Til slutt skal vi telle opp sammensetningene på formen $(0)^3$. En (0)-rad består av to inverspar, der elementene i de to inversparene genererer to ulike 2-torsjonselementer. Det finnes 12 mulige rader:



Figur 9.2: I figuren er to mulige sammensetninger av tre summer markert.

Vi kan tilsammen finne åtte tilsvarende sammensetninger av tre summer i figur 9.2.

Vi har nå funnet $1+6+6+8=21$ mulige strukturer av elementene i $\mathbb{Z}_4 \times \mathbb{Z}_4$ på formen

$$\begin{array}{cccc} 1 & 2 & 2 & 2 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{array}$$

9.2 Andre fordeling

Videre ønsker vi å finne antall måter å plassere elementene i fire summer sortert etter orden som dette:

$$\begin{array}{cccc} 1 & 4 & 4 & 4 \\ 2 & 4 & 4 & 4 \\ 2 & 4 & 4 & 4 \\ 2 & 4 & 4 & 4 \end{array}$$

Elementene som ikke er av orden 4 skal altså være i hver sin sum, og alle summene skal være null. Vi bruker fortsatt figur 9.1 for å systematisk telle opp antall muligheter. I $(0,0)$-raden må vi velge tre elementer fra ulike undergrupper av orden 8. Hvis vi for eksempel velger $(1,0)$ som første ledd i summen, kan vi verken velge $(3,0)$, $(1,2)$ eller $(3,2)$ som et av de andre to leddene. Mulighetene ved et valg at $(1,0)$ som et av leddene, blir disse summene:

$$\begin{aligned} (1,0)+(0,1)+(3,3) &= (0,0), \\ (1,0)+(2,1)+(1,3) &= (0,0), \\ (1,0)+(0,3)+(3,1) &= (0,0), \\ (1,0)+(2,3)+(1,1) &= (0,0). \end{aligned}$$

Tilsvarende finner vi fire summer ved valg av henholdsvis $(3,0)$, $(1,2)$ og $(3,2)$ som ledd i $(0,0)$-raden. Vi har dermed $4 \cdot 4 = 16$ muligheter.

I de neste radene skal tre elementer $a, b, c \in A$ velges slik at $\text{ord}(a+b+c) = 2$. Dersom $2a = 2b$ vil a og b enten være inverser eller være slik at $\text{ord}(a+b) = 2$. Da kan vi ikke finne noen c slik at $\text{ord}(a+b+c) = 2$. Dermed vet vi at de tre elementene alltid må velges fra tre ulike undergrupper av orden 8.

La nå første rad være $(0,0)+(1,0)+(0,1)+(3,3) = (0,0)$, og la elementet av orden 2 i den neste raden være $(0,2)$. Hvis vi velger de to neste elementene i summen, vil det siste elementet være gitt for at alle elementene i raden skal summeres til null. Vi har følgende muligheter:

$$\begin{aligned} (0,0) &= (0,2)+(1,2)+(2,1)+(1,3) \\ &= (0,2)+(1,2)+(0,3)+(3,1) \\ &= (0,2)+(1,2)+(2,3)+(1,1) \\ &= (0,2)+(3,0)+(2,1)+(3,1) \\ &= (0,2)+(3,0)+(0,3)+(1,3) \\ &= (0,2)+(3,0)+(2,3)+(3,3) \\ &= (0,2)+(3,2)+(2,1)+(3,3) \\ &= (0,2)+(3,2)+(0,3)+(1,1) \\ &= (0,2)+(3,2)+(2,3)+(3,1). \end{aligned}$$

Vi ser at to av disse ni mulighetene tvinger siste element til å være et som allerede er brukt. Vi står derfor igjen med sju muligheter for denne raden for hvert valg av $(0,0)$-rad.

Vi velger $(0,2)$-raden til å være $(0,2)+(1,2)+(2,1)+(1,3)$, og lar det neste orden 2-elementet være $(2,0)$. Vi får følgende muligheter:

$$\begin{aligned}(0,0) &= (2,0)+(3,0)+(0,3)+(3,1)\\ &= (2,0)+(3,0)+(2,3)+(1,1)\\ &= (2,0)+(3,2)+(0,3)+(3,3)\\ &= (2,0)+(3,2)+(2,3)+(1,3).\end{aligned}$$

Her er det to muligheter som tvinger det siste elementet til å være et vi allerede har valgt. Det er altså igjen to muligheter for denne raden, og av lemma 9.2 er vi trygge på at de siste fire elementene i A også legges sammen til null.

Vi har nå fått $16 \cdot 7 \cdot 2 \cdot 1 = 224$ mulige måter å strukturere elementene på når hver av de fire summene skal inneholde ett element som ikke er av orden 4.

9.3 Tredje fordeling

I det neste tilfellet skal vi la identiteten og ett element av orden 2 være i samme sum. De to andre 2-torsjonselementene skal være i hver sin sum, slik at en av summene kun inneholder elementer av orden 4:

$$\begin{array}{cccc}1 & 2 & 4 & 4\\ 2 & 4 & 4 & 4\\ 2 & 4 & 4 & 4\\ 4 & 4 & 4 & 4\end{array}$$

Vi har tre valg av orden 2-element til den øverste raden. Ved å bruke figur 9.1 kan vi for hvert av disse tre valgene finne fire muligheter.

Hvis vi for eksempel velger $(0,2)$ til øverste rad, må de to siste leddene summeres til $(0,2)$. Vi finner følgende:

$$\begin{aligned}(0,2) &= (1,0)+(3,2) = (1,2)+(3,0)\\ &= (1,1)+(3,1) = (1,3)+(3,3).\end{aligned}$$

Dermed har vi $3 \cdot 4 = 12$ valg for denne raden. Vi velger den øverste raden til å være $(0,0)+(0,2)+(1,0)+(3,2)$, og finner antall muligheter for neste rad. La det neste 2-torsjonselementet være $(2,0)$, slik at vi nå skal velge tre av de gjenværende elementene i A som tilsammen blir $(2,0)$. Siden vi allerede har

valgt to av elementene som genererer $(2,0)$, og vi må velge de tre leddene fra ulike undergrupper av orden 8, må et ledd være enten $(3,0)$ eller $(1,2)$. Hvert av disse valgene gir fire mulige summer, slik at vi tilsammen har åtte muligheter for denne raden. Av disse åtte velger vi $(2,0)+(1,2)+(0,1)+(1,1)$. Vi skal finne antall muligheter for summen med leddet $(2,2)$ når vi nå står igjen med sju elementer av orden 4: $(2,1)$, $(2,3)$, $(0,3)$, $(1,3)$, $(3,0)$, $(3,1)$ og $(3,3)$.Ved å velge blant disse, finner vi:

$$\begin{aligned}(2,2) &= (1,3)+(2,3)+(3,0)\\ &= (0,1)+(3,0)+(3,3).\end{aligned}$$

For raden som inneholder leddet $(2,2)$, har vi altså to muligheter.

Tilsammen får vi $12 \cdot 8 \cdot 2 \cdot 1 = 192$ mulige strukturerings av alle de 16 elementene på denne måten.

9.4 Fjerde fordeling

Nå vil vi finne antall måter å strukturere elementene som dette:

$$\begin{array}{cccc}1 & 2 & 4 & 4\\ 2 & 2 & 4 & 4\\ 4 & 4 & 4 & 4\\ 4 & 4 & 4 & 4\end{array}$$

Vi har allerede funnet ut at det finnes fire muligheter for hvert valg av 2-torsjonselement i den første raden. Vi gjør følgende observasjon:

Lemma 9.6. *Summen av to av elementene av orden* 2 *blir det tredje.*

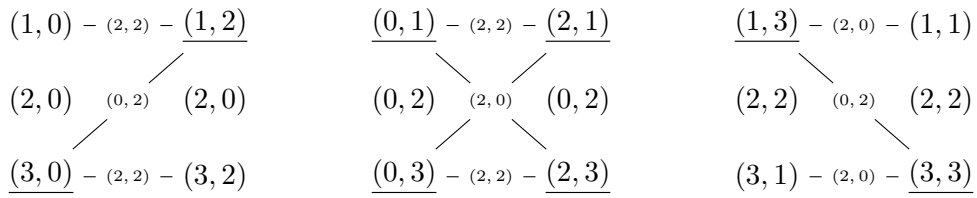
Bevis. Vi regner ut:

$$\begin{aligned}(2,0)+(0,2) &= (2,2),\\ (2,0)+(2,2) &= (0,2),\\ (0,2)+(2,2) &= (2,0).\end{aligned}$$ □

Andre rad vil derfor bli av samme type som første, og vi står igjen med tre valg. Ett av disse tre valgene gir orden 4-elementer fra samme undergruppe som de to i første rad, mens de to andre valgene gir elementer fra en annen undergruppe. Ved et bestemt valg av de to første radene, har vi igjen åtte elementer av orden 4 som skal fordeles i to summer. La først de to første radene være

$$\begin{aligned}&(0,0)+(0,2)+(1,0)+(3,2),\\ &(2,0)+(2,2)+(1,1)+(3,1).\end{aligned}$$

Her er altså de to parene av orden 4-elementer valgt fra to ulike undergrupper av orden 8. Vi står nå igjen med elementene markert i figuren under.



Hvis vi legger sammen to av de fire elementene fra undergruppen i midten, får vi enten $(0,0)$, $(2,2)$ eller $(2,0)$. Vi kan kun velge de to siste elementene her for å få en sum av fire ledd som skal bli null. Den eneste muligheten for å plassere de åtte elementene i to summer blir dermed:

$$(1,2)+(3,0)+(1,3)+(3,3),$$
$$(0,1)+(0,3)+(2,1)+(2,3).$$

Vi har dermed funnet $12 \cdot 2 \cdot 1 = 24$ muligheter til å strukturere elementene på denne måten.

Velg nå de to første radene til å inneholde elementer fra samme undergruppe:

$$(0,0)+(0,2)+(1,0)+(3,2),$$
$$(2,0)+(2,2)+(1,2)+(3,0).$$

Da står vi igjen med de åtte orden 4-elementene fra de to andre undergruppene. Ved å bruke figur 9.1, kan vi finne fem muligheter for de to siste radene:

- Det er én mulighet hvis vi velger to $(0,2,2)$-rader.
- Hvis vi lager to (0)-rader, finner vi to muligheter.
- Hvis vi lager to (2)-rader, finner vi to muligheter.

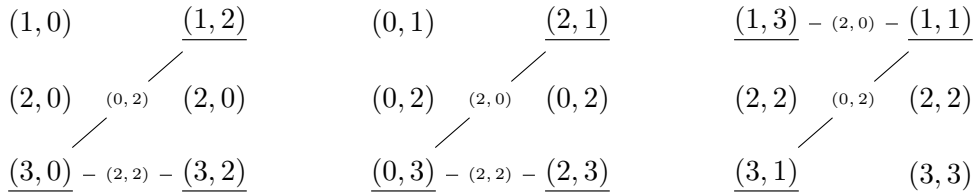
Siden et valg av type av én rad gjør at vi står igjen med elementer som danner en rad av samme type, finnes ingen andre muligheter enn disse. Dermed har vi funnet $12 \cdot 1 \cdot 5 = 60$ muligheter for å strukturere elementene, og $24+60 = 84$ tilsammen for denne måten å plassere elementene på etter orden.

9.5 Femte fordeling

Vi lar nå identitetselementet være i en rad uten 2-torsjonselementer, men plasserer disse på denne måten:

$$\begin{matrix} 1 & 4 & 4 & 4 \\ 2 & 2 & 4 & 4 \\ 2 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{matrix}$$

Vi har tidligere funnet 16 valg for første rad. Det er igjen ni elementer av orden 4 til de andre tre radene. La den første raden være $(0,0)+(1,0)+(0,1)+(3,3)$. De gjenværende elementene er markert i figuren under.



Vi har tre alternativer for valg av orden 2-elementer i andre rad. Velg $(0,2)$ og $(2,2)$. I figuren kan vi finne to måter å legge sammen to elementer til å bli $(2,0)$. Dermed får vi følgende muligheter for andre rad ved dette valget av elementer av orden 2:

$$(0,2)+(2,2)+(0,3)+(2,1),$$
$$(0,2)+(2,2)+(1,3)+(1,1).$$

Hvis vi velger den første av disse to, står vi igjen med sju elementer av orden 4: $(1,2)$, $(3,0)$, $(3,2)$, $(2,3)$, $(1,3)$, $(1,1)$ og $(3,1)$. Vi finner følgende muligheter for den tredje raden:

$$(2,0)+(3,0)+(2,3)+(1,1),$$
$$(2,0)+(3,2)+(2,3)+(1,3).$$

Dermed har vi funnet $16\cdot3\cdot2\cdot2\cdot1=192$ mulige struktureringer av elementene i $\mathbb{Z}_4\times\mathbb{Z}_4$.

9.6 Opptelling

Vi oppsummerer opptellingen i en tabell:

Strukturering av elementene				**Antall muligheter**
1	2	2	2	21
4	4	4	4	
4	4	4	4	
4	4	4	4	
1	4	4	4	224
2	4	4	4	
2	4	4	4	
2	4	4	4	
1	2	4	4	192
2	4	4	4	
2	4	4	4	
4	4	4	4	
1	2	4	4	84
2	2	4	4	
4	4	4	4	
4	4	4	4	
1	4	4	4	192
2	2	4	4	
2	4	4	4	
4	4	4	4	

Tabell 9.1: En oppsummering av opptellingen av antall plan.

Tilsammen har vi funnet 21+224+192+84+192 = 713 mulige måter å fordele de 16 elementene i fire nullsummer, og vi har dermed bevist teorem 9.1.

Kapittel 10

Geometrisk tolkning

Vi skal i dette kapitlet forklare hvordan man kan finne ut av hvilke av de hyperoskulerende punktene som er 2-torsjonspunkter, og hvilke som er 4-torsjonspunkter. Origo i H_4 kan velges fritt, og det er dette valget som bestemmer hvilke av de andre punktene som er 2-torsjonspunkter. Kall valget av origo for P_0.

Proposisjon 10.1. *Et punkt P på en elliptisk kurve E i $\mathbb{P}^3$ er et 2-torsjonspunkt dersom tangentlinja $T_P(E)$ skjærer tangentlinja $T_{P_0}(E)$.*

Bevis. Dersom et punkt P er et 2-torsjonspunkt, vil vi i gruppa av punkter på E ha $2P = P_0$. Da har vi også $2P \oplus 2P_0 = P_0$, som betyr at det finnes et plan π' som snitter E både i P og P_0 med snittmultiplisitet 2. Kall penselen av plan som inneholder tangentlinja i $P_i \in E$ for $\Omega_{P_i} = \{\pi | T_{P_i}(E) \subset \pi\}$. Da vil π' både være inneholdt i både Ω_P og Ω_{P_0}, slik at tangentlinjene til kurven i de to punktene snitter. Punktet P er i H_4 siden likheten $2P = P_0$ impliserer $4P = P_0$. □

Lemma 10.2. *Det finnes tre 2-torsjonspunkter på E.*

Bevis. Vi ønsker å finne ut av hvor mange punkter på E som har tangentlinje som skjærer $T_{P_0}(E)$. Vi ser på snittet mellom E og plan i Ω_{P_0}, som definerer et lineært system $\{\text{div}_E(\pi \cap E) | \pi \in \Omega_{P_0}\}$. Av dette kan vi definere en avbildning ϕ fra kurven til en projektiv linje L. Siden et plan fra Ω_{P_0} generelt snitter E i to andre punkter enn P_0, er graden til avbildningen 2.

La P' være et punkt på L. Hurwitz' formel (se kapittel 4.1) gir oss

$$\begin{aligned} 2g_E - 2 &= \deg \phi(2g_L - 2) + R_\phi, \\ 0 &= -4 + R_\phi, \\ R_\phi &= \sum_{P \in \phi^{-1}(P')} (e_P^\phi - 1) = 4. \end{aligned}$$

For punktene der planene i Ω_{P_0} snitter kurven dobbelt i kun ett punkt, vil fiberkoeffisienten være 2, slik at hvert av disse punktene gir bidrag 1 til ramifikasjonen til ϕ. Et av punktene som gir bidrag til ramifikasjonen er P_0 selv, slik at vi står igjen med tre andre punkter med fiberkoeffisient lik 2. Planet som snitter E dobbelt både i P_0 og et annet punkt P er da et tangentplan til begge punktene, slik at tangentlinjene i hvert punkt skjærer hverandre. □

Videre ønsker vi å finne en konstruksjon for å bestemme de andre hyperoskulerende punktene.

Proposisjon 10.3. *For hvert valg av 2-torsjonspunkt P_i, $i = 1, 2, 3$, vil linja $l_{P_0P_1}$ skjære tangentlinjene til fire 4-torsjonspunkter. Tilsammen har vi da funnet de $3 \cdot 4 = 12$ elementene av orden 4 i H_4.*

Bevis. Vi har hittil valgt et origo P_0 og tre 2-torsjonspunkter P_1, P_2 og P_3. Trekk en linje $l_{P_0P_1}$ fra P_0 til P_1. Penselen av plan gitt av denne linja vil generelt inneholde plan som snitter E i to andre punkter. Et endelig antall plan vil snitte E i ett punkt med snittmultiplisitet 2. I et slikt tilfelle, der et plan snitter kurven dobbelt i et punkt P_4, får vi $P_0 \oplus P_1 \oplus 2P_4 = P_0$. Da har $2P_4$ orden 2 i H_4, som betyr at P_4 er et 4-torsjonspunkt. Ved å bruke gruppeisomorfien $H_4 \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, vet vi at det er fire alternativer for P_4 dersom $\text{ord}(2P_4) = 2$. Dersom 2-torsjonspunktet for eksempel er representert ved $(2, 0)$, vil både $(1, 0)$, $(1, 2)$, $(3, 0)$ og $(3, 2)$ være løsninger for $2P_4 = (2, 0)$. Vi får tilsvarende like mange 4-torsjonspunkter for hvert valg av de andre to 2-torsjonspunktene, slik at vi tilsammen har funnet $3 \cdot 4 = 12$ punkter av orden 4, og dermed alle punktene i H_4. □

Avslutning

I denne oppgaven har vi studert undergruppene bestående av henholdsvis 3-torsjonspunkter på en elliptisk kurve i $\mathbb{P}^2$ og 4-torsjonspunkter på en elliptisk kurve i $\mathbb{P}^3$. Videre kunne det vært interessant å studere torsjonspunkter av høyere orden. Hver mengde $\{P \mid nP = P_0\}$ av n-torsjonspunkter er en undergruppe av gruppen av alle punktene på en elliptisk kurve. Vi kunne videre funnet en hyperflate som skjærer kurven i n-torsjonspunktene, for bestemte verdier av n, men eventuelt med høyere snittmultiplisitet i et gitt origo P_0.

Det hadde også vært nyttig å ta for seg eksplisitte elliptiske kurver for å se hvordan gruppeloven fungerer på gitte punkter. Da kunne vi også funnet uttrykk for en hyperflate som skjærer kurven i n-torsjonspunktene, for bestemte verdier av n, og koordinatene til disse punktene.

Bibliografi

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[3] John B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[4] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[5] Ragni Piene. Cuspidal projections of space curves. *Math. Ann.*, 256(1):95–119, 1981.

[6] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.